MATH 123. LECTURE NOTES AND HOMEWORK PROBLEMS

LEVENT ALPOGE, GURBIR DHILLON AND DENNIS GAITSGORY

1. Tuesday, January 29

1.1. The universal property of quotient modules.

1.1.1. Let R be a ring, M an R-module, and $M' \subset M$ an R-submodule. We consider the quotient module M/M' and the natural projection $\pi : M \to M/M'$. Precomposition with π defines a map

$$\mathrm{Hom}_R(M/M', N) \to \mathrm{Hom}_R(M, N). \tag{1.1}$$

For an R-module N, we consider the set $\mathrm{Hom}_R(M, N)$ and its subset

$$\mathrm{Hom}_R(M, N)_{\text{vanish on } M'} \subset \mathrm{Hom}_R(M, N)$$

that consists of the $\phi : M \to N$ such that $\phi|_{M'} = 0$.

It is easy to see that the image of the map (1.1) belongs to $\mathrm{Hom}_R(M, N)_{\text{vanish on } M'}$. Hence, we obtain a map

$$\mathrm{Hom}_R(M/M', N) \to \mathrm{Hom}_R(M, N)_{\text{vanish on } M'}. \tag{1.2}$$

Proposition 1.1.2. *The map* (1.2) *is a bijection.*

Proof. We construct a map

$$\mathrm{Hom}_R(M, N)_{\text{vanish on } M'} \to \mathrm{Hom}_R(M/M', N), \tag{1.3}$$

which we will eventually prove to be the inverse of (1.2), as follows.

Given $\phi : M \to N$ with $\phi|_{M'} = 0$, we attach to it the following map

$$\psi : M/M' \to N.$$

For an element $\overline{m} \in M/M'$, choose $m \in M$ such that $\pi(m) = \overline{m}$. Set

$$\psi(\overline{m}) := \phi(m).$$

First, we need to show that the assignment

$$\overline{m} \mapsto \psi(\overline{m})$$

is well-defined, i.e., is independent of the choice of m with $\pi(m) = \overline{m}$. Indeed, if

$$\pi(m_1) = \overline{m} = \pi(m_2),$$

by the definition of M/M', there exists $m' \in M'$ such that $m_1 = m_2 + m'$. But then

$$\phi(m_1) = \phi(m_2) + \phi(m') = \phi(m_2),$$

by the vanishing condition on ϕ, as desired.

Thus, we obtain that ψ is well-defined as a map of sets $M/M' \to N$. We now need to check that ψ is a map of R-modules. We will only check that it is R-linear;

the fact that it is additive is checked similarly. For $r \in R$ and $\overline{m} \in M/M'$ we need to check that

$$\psi(r \cdot \overline{m}) = r \cdot \psi(\overline{m}).$$

Let $m \in M$ be as above. Then $\pi(r \cdot m) = r \cdot \overline{m}$. Hence, by the construction of ψ, (since we are free to choose *any* lift of $r \cdot \overline{m}$ we can find, for instance rm)

$$\psi(r \cdot \overline{m}) = \phi(r \cdot m),$$

while $r \cdot \psi(\overline{m}) = r \cdot \phi(m)$. Now, the desired equality follows from the equality

$$\phi(r \cdot m) = r \cdot \phi(m),$$

which holds since ϕ is an R-module homomorphism.

We now need to check that the maps (1.2) and (1.3) are mutually inverse.

We first check that the composition (1.2) $\circ$ (1.3) equals the identity map on the set $\mathrm{Hom}_R(M,N)_{\text{vanish on } M'}$. Starting from $\phi \in \mathrm{Hom}_R(M,N)_{\text{vanish on } M'}$ we let $\psi \in \mathrm{Hom}_R(M/M',N)$ be its image under the map (1.3). We need to show that $\phi = \psi \circ \pi$, i.e., that for every $m \in M$, we have $\phi(m) = \psi \circ \pi(m)$. However, for $m \in M$, we have $\psi \circ \pi(m) := \psi(\pi(m)) = \phi(m)$, by the construction of ψ (since m is a lift of $\pi(m)$), as desired.

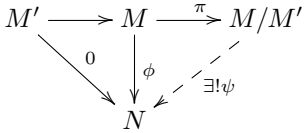
We now check that the composition (1.3) $\circ$ (1.2) equals the identity map on the set $\mathrm{Hom}_R(M/M',N)$. Starting from $\psi \in \mathrm{Hom}_R(M/M',N)$, let $\widetilde{\psi}$ be the image of the map $\phi := \psi \circ \pi$ under (1.3). We need to check that $\widetilde{\psi} = \psi$, i.e., that for every $\overline{m} \in M/M'$, we have $\widetilde{\psi}(\overline{m}) = \psi(\overline{m})$. Choose $m \in M$ with $\pi(m) = \overline{m}$. Then $\widetilde{\psi}(\overline{m}) := \phi(m) := \psi \circ \pi(m) = \psi(\overline{m})$, as desired.

□

It's worth saying that the above looks like a tautology (note the number of ":="s that appeared) because it essentially is: we have only reorganized what we've already said about the quotient module into the above.

1.1.3. Note that Proposition 1.1.2 can be reformulated as follows:

Corollary 1.1.4. *For any map (of R-modules) $\phi : M \to N$ with $\phi|_{M'} = 0$ there exists a unique map (of R-modules) $\psi : M/M' \to N$ such that $\phi = \psi \circ \pi$.*



We can phrase the above corollary in words as follows:

For a map $\phi : M \to N$, a necessary and sufficient condition that it factor through π is that $\phi|_{M'} = 0$. If this condition holds, then the factorization in question is unique.

1.2. **The free R-module.** Consider R as a module over itself. Consider the map of sets

$$\mathrm{Hom}_R(R, M) \to M \tag{1.4}$$

that sends $\phi : R \to M$ to the element $\phi(1) \in M$.

Proposition 1.2.1. *The map* (1.4) *is a bijection.*

Proof. We construct a map

$$M \to \mathrm{Hom}_R(R, M) \tag{1.5}$$

as follows. To an element $m \in M$ we assign a map $\phi : R \to M$ defined by

$$\phi(r) = r \cdot m.$$

Week 1, Problem 1.[1] *Show that ϕ defined in the above way is an R-module homomorphism. Show that the maps* (1.4) *and* (1.5) *are mutually inverse.* □

1.2.2. We can rephrase Proposition 1.2.1 as follows:

Corollary 1.2.3. *For every element $m \in M$ there exists a unique map (of R-modules) $\phi : R \to M$ such that $\phi(1) = m$.*

1.3. **Direct sums.** The material of this subsection was not explicitly presented in class. Recall the notion of direct sum we played with last semester. In the spirit of finding a universal property for every construction we know, let's proceed to find one for the direct sum. But first, a (slightly more general) definition of the direct sum we'd seen.

1.3.1. Let A be a (possibly infinite) set, and let M_a be an R-module assigned to each element $a \in A$. We define the direct sum

$$\bigoplus_{a \in A} M_a$$

to be the set of all assignments

$$\underline{m} : a \mapsto m_a \in M_a, \quad \forall a \in A,$$

subject to the condition that, *for all but finitely many elements $a \in A$*, we have $m_a = 0$.

Equivalently, $\bigoplus_{a \in A} M_a$ is the set of all formal expressions

$$\sum_{a \in A} m_a,$$

where $m_a \in M_a$, and $m_a = 0$ *for all but finitely many elements $a \in A$*.

The structure of R-module on $\bigoplus_{a \in A} M_a$ is componentwise. E.g., for $r \in R$ and $\underline{m} \in \bigoplus_{a \in A} M_a$ corresponding to $a \mapsto m_a$, the element $r \cdot \underline{m}$ is defined to be the assignment $a \mapsto r \cdot m_a$ (check that this makes $\bigoplus_{a \in A} M_a$ into an R-module).

For example, if all M_a are taken to be the same module M, we obtain the R-module denoted $M^{\oplus A}$.

[1] Do not do this problem if you have done it in the framework of another class.

1.3.2. As an example, if $A = \mathbb{Z}$, the resulting direct sum

$$\bigoplus_{n\in\mathbb{Z}} M_n$$

is precisely the set of tuples

$$\{(m_n)_{n\in\mathbb{Z}} :\ m_n = 0 \text{ for all but finitely many } n\},$$

endowed with componentwise addition and scalar multiplication. Or, if A is finite, this is precisely the finite direct sum we've already come to know and love. Thanks to these examples, oftentimes one also uses the notation $(m_a)_{a\in A}$ for an element of $\bigoplus_{a\in A} M_a$.

1.3.3. For every element $b \in A$ we have an R-module homomorphism

$$i_b : M_b \to \bigoplus_{a\in A} M_a,$$

defined by sending $m_b \in M_b$ to the assignment

$$a \mapsto \begin{cases} m_b & a = b, \\ 0 & a \neq b. \end{cases}$$

In the case of A a two element set, this map is precisely $M \mapsto M \oplus N$ via $m \mapsto (m, 0)$.

1.3.4. For an R-module N, consider the map of sets

$$\mathrm{Hom}_R\left(\bigoplus_{a\in A} M_a, N\right) \to \prod_{a\in A} \mathrm{Hom}_R(M_a, N) \tag{1.6}$$

that sends $\phi \in \mathrm{Hom}_R(\bigoplus_{a\in A} M_a, N)$ to the element $\underline{\phi} \in \prod_{a\in A} \mathrm{Hom}_R(M_a, N)$ that takes

$$a \mapsto \underline{\phi}(a) := \phi_a := \phi \circ i_a.$$

Proposition 1.3.5. *The map* (1.6) *is a bijection.*

Proof. We construct a map

$$\prod_{a\in A} \mathrm{Hom}_R(M_a, N) \to \mathrm{Hom}_R\left(\bigoplus_{a\in A} M_a, N\right) \tag{1.7}$$

as follows.

Given

$$\underline{\phi} \in \prod_{a\in A} \mathrm{Hom}_R(M_a, N), \quad a \mapsto \phi_a \in \mathrm{Hom}_R(M_a, N),$$

we assign to it the map

$$\phi : \bigoplus_{a\in A} M_a \to N$$

for which, given $\underline{m} \in \bigoplus_{a\in A} M_a$ (specified by $m_a \in M_a$), we set

$$\phi(\underline{m}) := \sum_{a\in A} \phi_a(m_a),$$

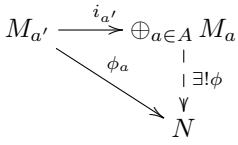
where the sum is finite because of the condition on $\underline{m}$ (namely, that $m_a = 0$ for all but finitely many a).

Week 1, Problem 2.[2] *Show that ϕ defined in the above way is an R-module homomorphism. Show that the maps* (1.6) *and* (1.7) *are mutually inverse.*

□

1.3.6. We can rephrase Proposition 1.3.5 as follows:

Corollary 1.3.7. *For every collection of maps (of R-modules) $\phi_a : M_a \to N$ there exists a unique map (of R-modules) $\phi : \bigoplus_{a \in A} M_a \to N$ such that $\phi_a = \phi \circ i_a$ for every $a \in A$.*



That is to say, to give a map $\bigoplus_{a \in A} M_a \to N$ is precisely equivalent to giving maps out of each $M_a \to N$.

1.3.8. For example, take all $M_a = R$. Define $e^a \in R^{\oplus A}$ by

$$e^a(a') = \begin{cases} 1 & a' = a, \\ 0 & a' \neq a. \end{cases}$$

Note that we can think of $R^{\oplus A}$ as the set of all expressions

$$\sum_{a \in A} r_a \cdot e^a,$$

where $r_a = 0$ for all but finitely many elements $a \in A$. Often these are written as "A-tuples" $(r_a)_{a \in A}$, where addition and scalar multiplication are performed entrywise.

Combining Corollaries 1.3.7 and 1.2.3, we obtain:

Corollary 1.3.9. *For every collection of elements*

$$\underline{n} \in N^{\times A}, \quad a \mapsto n_a \in N,$$

there exists a unique map of R-modules

$$\phi : R^{\oplus A} \to N,$$

such that $\phi(e^a) = n_a$.

That is to say, giving a map out of a free module with basis indexed by A is precisely equivalent to giving points of N indexed by A: i.e., to say where the basis goes.

1.4. **The submodule generated by a given set of elements.**

[2]Do not do this problem if you have done it in the framework of another class.

1.4.1. Let M be an R-module, and $m_a \in M$ be a collection of elements of M parameterized by a set A. We let

$$R \cdot \{m_a \mid a \in A\} := \sum_{a \in A} R \cdot m_a$$

denote the subset of elements of M that can be written as finite linear combinations of the m_a's, i.e., as sums

$$\sum_{a \in A} r_a \cdot m_a,$$

where r_a are nonzero for only finitely many $a \in A$.

Lemma 1.4.2. *The submodule $R \cdot \{m_a | a \in A\}$ is the minimal among (i.e., contained in all) R-submodules of M that contain all the elements m_a.*

Proof. Do it yourself! □

1.4.3. Consider the element $\underline{m} \in M^{\times A}$ given by $a \mapsto m_a$. Let $\phi_{\underline{m}} : R^{\oplus A} \to M$ be the R-module homomorphism corresponding to $\underline{m}$ by Corollary 1.3.9.

Lemma 1.4.4. $R \cdot \{m_a | a \in A\} = \mathrm{Im}(\phi_{\underline{m}})$.

Proof. Do it yourself! □

1.4.5. The following (useful) assertion is very easy:

Lemma 1.4.6. *Let $\phi : M \to N$ be a map of R-modules, such that $\phi(m_a) = 0$ for every $a \in A$. Then $\phi|_{M'} = 0$ for $M' = R \cdot \{m_a | a \in A\}$.*

2. Thursday, January 31

2.1. **Modules given by generators and relations.** The contents of this subsection were not expicitly in the lecture.

2.1.1. Let us return to the set-up of Sect. 1.3.8. I.e., we have a set A, and we consider the R-module $R^{\oplus A}$.

Let B be another set, and let us be given a map of R-modules

$$T : R^{\oplus A} \to R^{\oplus B}.$$

Note that by Corollary 1.3.9, the datum of T amounts to specifying an array (or, more familiarly, a matrix) of elements of R, parameterized by elements of the set $A \times B$:

$$(a, b) \mapsto r_{a,b},$$

with the property that for every b, there exists only finitely many a's, for which $r_{a,b} \neq 0$.

In other words, if $\{e^a\}$ is the standard basis for $R^{\oplus A}$, and $\{f^b\}$ is the standard basis for $R^{\oplus B}$, we have

$$T(e^a) = \sum_{b \in B} r_{a,b} \cdot f^b. \tag{2.1}$$

2.1.2. Now consider the module

$$M := R^{\oplus B}/\operatorname{Im}(T).$$

Let π denote the tautological projection

$$R^{\oplus B} \to M.$$

Let $m_b := \pi(f^b)$.

Under the above circumstances we shall say that the module M is *given by the generators* $\{m_b | b \in B\}$ *and the relations*

$$\sum_{b \in B} r_{a,b} \cdot m_b = 0, \quad \forall\, a \in A.$$

Note that the equations

$$\sum_{b \in B} r_{a,b} \cdot m_b = 0$$

imply yet more equations of this type: take e.g. linear combinations of finitely many of these relations to get others. This is why we must quotient out by $\operatorname{Im}(T)$, the submodule of $R^{\oplus B}$ generated by these sums.

2.1.3. In other words, when we say that a module M given by generators and relations, we specify

- a set B,
- a map $B \to M$, $b \mapsto m_b$,
- another set A,
- a map $A \times B \to R$, $a, b \mapsto r_{a,b}$, such that for every a, there exists only finitely many b's for which $r_{a,b} \neq 0$,

such that

- the map $R^{\oplus B} \xrightarrow{\pi} M$, $f^b \mapsto m_b$ is surjective,
- the composition $R^{\oplus A} \xrightarrow{T} R^{\oplus B} \xrightarrow{\pi} M$ is 0, where T is defined by (2.1),
- and the resulting map $R^{\oplus A} \to \ker(\pi)$ is surjective.

Week 1, Problem 3. *Show that* any *module can be given by generators are relations.*

For example, the $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ is given by the generator $\bar{1}$, and relation $2 \cdot \bar{1} = 0$. That is to say, the map $2\cdot : \mathbb{Z} \to \mathbb{Z}$ via multiplication by 2 produces $\mathbb{Z}/2\mathbb{Z}$ as $\mathbb{Z}/\operatorname{Im}(2\cdot)$. As another example, the module $R^{\oplus A}$ is given by the generators e^a and *no* relations. This is why it is called a *free* module: the generators are free to do as they please.

2.1.4. Let M be as above, and let N be another R-module. Let $A \to N$ via $a \mapsto n_a$.

The following statement results from combining Corollary 1.3.9, Corollary 1.1.4 and Lemma 1.4.6:

Corollary 2.1.5. *There exists a map*

$$\phi : M \to N, \quad \phi(m_a) = n_a$$

if and only if

$$\sum_{a \in A} r_{a,b} \cdot n_a = 0, \quad \forall\, b \in B.$$

If it exists, such a map is unique.

We can phrase this corollary in words as follows:

If a module is given by generators and relations, a map out of it is uniquely determined by specifying the map's value on the generators. Such a map exists if and only if the relations are satisfied in the target.

That is to say, the only constraint to mapping out of a module given by a bunch of generators is that all the relations satisfied in the domain have to continue to hold in the target. So, for instance, an intrepid homomorphism-producer might try to produce a map $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$ by writing down the image of $\bar{1} \in \mathbb{Z}/2\mathbb{Z}$, say $a \in \mathbb{Z}$. But, unfortunately, the relation $2 \cdot \bar{1} = 0$ must continue to hold, which forces $2a = 0$ — i.e., $a = 0$. So the only $\mathbb{Z}$-module map from $\mathbb{Z}/2\mathbb{Z}$ to $\mathbb{Z}$ is the zero map.

2.2. **Tensor products: construction.** OK. So we have built up foundations this far almost entirely because of what follows. But perhaps some motivation is in order.

First, multilinear objects are ubiquitous in mathematics. But one could say that this is because of the success of the theory to follow. In any case, if you have ever considered the standard inner product on $\mathbb{R}^n$, and what might happen if you played around with the coordinates, or what actually happens mathematically when you take a matrix over $\mathbb{R}$ and "regard" it as a complex matrix (and then manipulate as necessary, e.g. by finding an eigenvalue or playing with it otherwise), you have seen the results of a behind-the-scenes tensor product.

You might wonder if there is a space inside which these inner products (or similar objects) live: perhaps you've seen the "skew-symmetric" brand of inner product that flips a sign when you switch the two inputs, or perhaps you've wondered about degenerate pairings, etc. Of course, once you write down coordinates, everything becomes a matrix, but there is a more intrinsic way of writing down the space of such "bilinear" operations (just like we wrote down Hom without appealing to matrices) called the *tensor product*.

2.2.1. Let M be a right R-module, and N a left R-module. We are going to define an abelian group, denoted

$$M \underset{R}{\otimes} N,$$

and called the *tensor product of M and N over R*.

Do keep in mind that an abelian group is the same as a module for the ring $\mathbb{Z}$. We shall carry out the construction of $M \underset{R}{\otimes} N$ *as a $\mathbb{Z}$-module* in the framework of Sect. 2.1.

We let $M \underset{R}{\otimes} N$ be generated by elements denoted

$$m \otimes n, \quad m \in M, \quad n \in N.$$

I.e., the set A is $M \times N$.

We impose the following relations:

$$(m_1 + m_2) \otimes n - m_1 \otimes n - m_2 \otimes n = 0; \quad m_1, m_2 \in M, n \in N$$

$$m \otimes (n_1 + n_2) - m \otimes n_1 - m \otimes n_1 = 0; \quad m \in M, n_1, n_2 \in N;$$

$$(m \cdot r) \otimes n - m \otimes (r \cdot n) = 0; \quad m \in M, n \in N, r \in R.$$

Note that these are the generalizations of the bilinearity relations. The only strange one is this $(m \cdot r) \otimes n = m \otimes (r \cdot n)$ guy, but in fact this is the correct generalization of "bilinearity" to the setting of an arbitrary ring.

I.e. (if you insist on following the above discussions precisely!), the set B is the disjoint union

$$(M \times M \times N) \sqcup (M \times N \times N) \sqcup (M \times R \times N),$$

and the elements $r_{a,b}$ are as follows:

- For $b = (m_1, m_2, n) \in M \times M \times N$,

$$a = \begin{cases} 1 & a = (m_1 + m_2, n), \\ -1 & a = (m_1, n), \\ -1 & a = (m_2, n), \\ 0 & \text{otherwise.} \end{cases}$$

- For $b = (m, n_1, n_2) \in M \times N \times N$,

$$a = \begin{cases} 1 & a = (m, n_1 + n_2), \\ -1 & a = (m, n_1), \\ -1 & a = (m, n_2), \\ 0 & \text{otherwise.} \end{cases}$$

- For $b = (m, r, n) \in M \times R \times N$,

$$a = \begin{cases} 1 & a = (m \cdot r, n), \\ -1 & a = (m, r \cdot n), \\ 0 & \text{otherwise.} \end{cases}$$

2.2.2. In other words, $M \underset{R}{\otimes} N$ is the abelian group ($\mathbb{Z}$-module) obtained as Q/Q', where $Q := \mathbb{Z}^{M \times N}$ with basis elements $e^{m,n}$, and Q' is the abelian subgroup generated by elements

$$e^{m_1+m_2,n} - e^{m_1,n} - e^{m_2,n}, \quad e^{m,n_1+n_2} - e^{m,n_1} - e^{m,n_2}, \quad e^{m \cdot r,n} - e^{m,r \cdot n}.$$

We denote by $m \otimes n$ the image of the basis element $e^{m,n}$ under the natural projection

$$Q \to Q/Q' =: M \underset{R}{\otimes} N.$$

2.2.3. Do not worry if the above is a bit bewildering. It is an instance in which the construction of an object is disgusting, but the particular property the object satisfies (which makes it "universal" among objects satisfying this property) is clean. In fact simply knowing the universal property is enough for one's purposes: the above will just be a proof of existence. But psychologically it is also easier to be able to think about the explicit construction, too.

2.3. **Tensor products: the universal property.**

2.3.1. Applying Corollary 2.1.5, we obtain:

Corollary 2.3.2. *For an abelian group P, a map $\phi : M \underset{R}{\otimes} N \to P$ is completely determined by its value on the elements $m \otimes n \in M \underset{R}{\otimes} N$. Such a map exists if and only if the following relations hold:*

$$\phi((m_1 + m_2) \otimes n) = \phi(m_1 \otimes n) + \phi(m_2 \otimes n),$$

$$\phi(m \otimes (n_1 + n_2)) = \phi(m \otimes n_1) + \phi(m \otimes n_1),$$

$$\phi((m \cdot r) \otimes n) = \phi(m \otimes (r \cdot n)).$$

2.3.3. Let P be an abelian group. We give the following definition:

Definition 2.3.4. *A R-bilinear pairing on $M \times N$ with values in P is a map of sets $M \times N \to P$ is a map of sets such that*

$$B((m_1 + m_2), n) = B(m_1, n) + B(m_2, n);$$

$$B(m, (n_1 + n_2)) = B(m, n_1) + B(m, n_1);$$

$$B((m \cdot r), n) = B(m, (r \cdot n)).$$

Note that if $B : M \times N \to P$ is a bilinear pairing and $\phi : P \to P'$ is a homomorphism of abelian groups, then $\phi \circ B : M \times N \to P'$ is a bilinear pairing on $M \times N$ with values in P'.

2.3.5. We define the bilinear pairing

$$B_{univ} : M \times N \to M \underset{R}{\otimes} N$$

by $B_{univ}(m, n) = m \otimes n$. Note that it is, in fact, bilinear, just because of the relations we imposed in the construction. Actually, the point is that we imposed the absolute *minimal* set of relations to make this pairing bilinear: this will make this pairing "universal" (hence the name B_{univ}).

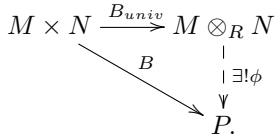
The following assertion expresses this universal property of the tensor product:

Proposition 2.3.6. *For an abelian group P, the assignment $\phi \mapsto \phi \circ B_{univ}$ is a bijection between $\mathrm{Hom}_{Ab}(M \underset{R}{\otimes} N, P)$ and the set of bilinear maps $B : M \times N \to P$.*

Week 1, Problem 4. *Deduce Proposition 2.3.6 from Corollary 2.3.2.*

Note that we can rephrase Proposition 2.3.6 as follows:

For any bilinear pairing $B : M \times N \to R$ there exists a unique map $\phi : M \underset{R}{\otimes} N \to P$ such that $B = \phi \circ B_{univ}$ — i.e., such that the following diagram commutes:



2.4. **Tensor products: basic properties.**

2.4.1. *Tensor product with the free module.* Let us take $N = R$. Consider the map

$$M \underset{R}{\otimes} R \to M, \quad \phi(m \otimes r) = m \cdot r. \tag{2.2}$$

This map is well-defined by Corollary 2.3.2.

Proposition 2.4.2. *The map* (2.2) *is an isomorphism of abelian groups.*

Proof. We construct a map

$$M \to M \underset{R}{\otimes} R \tag{2.3}$$

by sending $m \mapsto m \otimes 1$.

Week 1, Problem 5. *Show that the map* (2.3) *is a homomorphism of abelian groups, and that it provides an inverse to* (2.2).

□

Of course, a similar story occurs for $R \underset{R}{\otimes} N$, where R is considered as a *right* R-module via multiplication on the right.

2.4.3. *Functoriality.* Let $\phi : N_1 \to N_2$ be a map of left R-modules.

Lemma 2.4.4. *There exists a uniquely defined map of abelian groups*

$$M \underset{R}{\otimes} N_1 \to M \underset{R}{\otimes} N_2,$$

denoted $\mathrm{id}_M \otimes \phi$*, characterized by the property that*

$$(\mathrm{id}_M \otimes \phi)(m \otimes n_1) = (m \otimes \phi(n_1)).$$

In pictures:

$$\begin{array}{ccc} M \times N_1 & \xrightarrow{(id,\phi)} & M \times N_2 \\ \downarrow{\scriptstyle B_{univ}} & & \downarrow{\scriptstyle B_{univ}} \\ M \underset{R}{\otimes} N_1 & \xrightarrow{\exists!} & M \underset{R}{\otimes} N_2 \end{array}$$

Week 1, Problem 6. *Prove Lemma 2.4.4.*

Again, the same story occurs for maps $M_1 \to M_2$.

2.4.5. *Tensor products and direct sums.* Let A be a set, and $a \rightsquigarrow N_a$ a collection of R-modules. For each $a' \in A$, let $i_{a'}$ denote the corresponding map

$$N_{a'} \to \bigoplus_{a \in A} N_a.$$

By Lemma 2.4.4, for every $a' \in A$ we obtain a map

$$M \underset{R}{\otimes} N_{a'} \to M \underset{R}{\otimes} \left(\bigoplus_{a \in A} N_a \right).$$

By Proposition 1.3.5, we obtain a map

$$\bigoplus_{a \in A} (M \underset{R}{\otimes} N_a) \to M \underset{R}{\otimes} \left(\bigoplus_{a \in A} N_a \right). \tag{2.4}$$

Proposition 2.4.6. *The map* (2.4) *is an isomorphism.*

Proof. We define a map

$$M \underset{R}{\otimes} \left(\bigoplus_{a \in A} N_a \right) \to \bigoplus_a (M \underset{R}{\otimes} N_a) \tag{2.5}$$

via:

$$m \otimes (\sum_{a \in A} n_a) \in M \underset{R}{\otimes} \left(\bigoplus_{a \in A} N_a \right)$$

to the element

$$\sum_{a \in A} m \otimes n_a \in \bigoplus_{a \in A} (M \underset{R}{\otimes} N_a).$$

Note that we have only defined this map on the "simple tensors" (also called "elementary tensors" or "pure tensors") — i.e., the generators.

Week 1, Problem 7. *Show that the map* (2.5) *is well-defined (that is, check that the relations hold), and provides an inverse to* (2.4).

□

Again, the same story occurs when we interchange the roles of M and N.

2.5. **Tensor products and cokernels.**

2.5.1. *Terminology.* Let $\phi : M_1 \to M_2$ be a map of R-modules. The cokernel of ϕ, denoted $\mathrm{coker}(\phi)$ is by definition the R-module $M_2/\mathrm{Im}(\phi)$.

2.5.2. Let $\phi : N_1 \to N_2$ be a map of left R-modules. Set $N := \mathrm{coker}(\phi)$, and the let π denote the tautological map $N_2 \to N$.

By Lemma 2.4.4, we have canonically defined maps

$$(\mathrm{id}_M \otimes \phi) : M \underset{R}{\otimes} N_1 \to M \underset{R}{\otimes} N_2 \text{ and } (\mathrm{id}_M \otimes \pi) : M \underset{R}{\otimes} N_2 \to M \underset{R}{\otimes} N.$$

Moreover, it is easy to see that the composition $(\mathrm{id}_M \otimes \pi) \circ (\mathrm{id}_M \otimes \phi)$ is zero, since $\pi \circ \phi = 0$.

Hence, by Corollary 1.1.4, we obtain a map

$$\mathrm{coker}(\mathrm{id}_M \otimes \phi) \to M \otimes \mathrm{coker}(\phi). \tag{2.6}$$

Proposition 2.5.3. *The map* (2.6) *is an isomorphism.*

Proof. We define a map

$$M \underset{R}{\otimes} \mathrm{coker}(\phi) \to \mathrm{coker}(\mathrm{id}_M \otimes \phi), \tag{2.7}$$

as follows.

For $n \in N$ let $n_2 \in N_2$ be such that $\pi(n_2) = n$. We let the map (2.7) send $m \otimes n \in M \underset{R}{\otimes} N$ to the image of

$$m \otimes n_2 \in M \underset{R}{\otimes} N_2$$

under the tautological projection

$$\psi : M \underset{R}{\otimes} N_2 \to \mathrm{coker}(\mathrm{id}_M \otimes \phi).$$

Week 1, Problem 8. *Show that the assignment $m \otimes n \mapsto \psi(m \otimes n_2)$ does not depend on the choice of n_2 and hence gives rise to a well-defined map in* (2.7)*, which is inverse to the map* (2.6)*.*

□

Of course, again the same story applies when we interchange the roles of M and N.

2.5.4. *Algorithm for computing tensor products.* Note that combining Proposition 2.5.3, Proposition 2.4.6, Proposition 2.4.2, and Problem 3, we obtain the following algorithm for computing the tensor product $M \underset{R}{\times} N$:

Choose a presentation of N by generators and relations. I.e., write it as the cokernel of a map

$$T : R^{\oplus A} \to R^{\oplus B}, \quad T(e^a) = \sum_{b \in B} r_{a,b} \cdot f^b.$$

Consider the corresponding map

$$\mathrm{id}_M \otimes T : M \underset{R}{\otimes} R^{\oplus A} \to M \underset{R}{\otimes} R^{\oplus B}.$$

Using Propositions 2.4.6 and 2.4.2, we identify

$$M \underset{R}{\otimes} R^{\oplus A} \simeq M^{\oplus A}, \quad M \underset{R}{\otimes} R^{\oplus B} \simeq M^{\oplus B}.$$

Week 1, Problem 9. *Show that, under the above identifications, the map* $\mathrm{id}_M \otimes T$*, viewed as a map $M^{\oplus A} \to M^{\oplus B}$, sends the element $m \in M$ (thought of as an element of $M^{\oplus A}$ via $M \overset{i_a}{\hookrightarrow} M^{\oplus A}$) to the element of $M^{\oplus B}$, whose b-th coordinate is $m \cdot r_{a,b}$.*

2.5.5. *Some concrete computations.* Let $I \subset R$ be a left ideal, and consider the left R-module R/I.

Week 1, Problem 10.

(a) *Show that, for any right R-module M, the tensor product $M \underset{R}{\otimes} R/I$ is the abelian group equal to the quotient of M by the abelian subgroup $M \cdot I$ (denoted M/MI), generated by the elements $m \cdot i$ for each $m \in M$ and $i \in I$.*

(b) *Now compute* $(\mathbb{Z}/2\mathbb{Z}) \underset{\mathbb{Z}}{\otimes} (\mathbb{Z}/3\mathbb{Z})$.

3. Tuesday, February 5

Problem-solving session.

4. Thursday, February 7

4.1. **Tensoring up.** In this subsection we fix a pair of rings R_1 and R_2 and a ring homomorphism $\phi : R_1 \to R_2$.

4.1.1. The homomorphism ϕ allows us to view an R_2-module N as an R_1-module by

$$r_1 \cdot n := \phi(r_1) \cdot n, \quad r_1 \in R_1, n \in N.$$

This is called *restricting scalars*, or restriction for short.

The question we will address in this subsection is how, starting from an R_1-module M, we can produce an R_2-module. That is to say, how we might *extend scalars* from R_1 to R_2. (Think of taking a real vector space and making it a complex vector space: one simply has to find a way to multiply by i, and the clever way to do it is to just emulate the construction of $\mathbb{C}$ from $\mathbb{R}$: just take your vector space V and direct sum the thing with a new vector space called "iV", with the obvious relations! — e.g., $i \cdot$ "$iv'' = -v, i \cdot v =$ "iv'', etc. This sort of trick is captured by the tensor product.)

4.1.2. Let us regard R_2 as a *right* R_1-module via

$$r_2 \cdot r_1 := r_2 \cdot \phi(r_1).$$

For a left R_1-module M, consider the abelian group.

$$R_2 \underset{R_1}{\otimes} M.$$

The claim is that $R_2 \underset{R_1}{\otimes} M$ has a natural left R_2-module structure. Indeed, for $r,r_2' \in R_2$ and $m \in M$, we let

$$r_2' \cdot (r_2 \otimes m) := r_2' \cdot r_2 \otimes m. \tag{4.1}$$

Note that we have only specified the action on the pure tensors of $R_2 \underset{R_1}{\otimes} M$, so there is something to check: namely, that the action actually makes sense on the whole tensor product (i.e., satisfies the relevant relations).

But first, we need to show that the assignment (4.1) is a well-defined map of abelian groups $R_2 \underset{R_1}{\otimes} M \to R_2 \underset{R_1}{\otimes} M$! For this we note that the map

$$r_2 \mapsto r_2' \cdot r_2$$

is a homomorphism of *right* R_1-modules (this is the ubiquitous fact that multiplication on the left commutes with multiplication on the right), and the well-definedness of (4.1) follows from Lemma 2.4.4.

Next, we need to show that (4.1) indeed defines an action of R_2 on $R_2 \underset{R_1}{\otimes} M$. This amounts to showing the following.

- For $r_2', r_2'' \in R_2$, we have that
$$r_2' \cdot (r_2'' \cdot \star) = (r_2' \cdot r_2'') \cdot \star;$$
- For $r_2', r_2'' \in R_2$ and $n \in R_2 \underset{R_1}{\otimes} M$, we have
$$(r_2' \cdot \star) + (r_2'' \cdot \star) = (r_2' + r_2'') \cdot \star;$$
- $1 \cdot \star = \star$.

In each case, we are dealing with a map of abelian groups $R_2 \underset{R_1}{\otimes} M \to R_2 \underset{R_1}{\otimes} M$. Hence, the required identity is enough to check on the generators of $R_2 \underset{R_1}{\otimes} M$. That is to say, we had might as well take $\star := r_2 \otimes m$. In this case, the required identity is straightforward. For example,

$$\begin{aligned} r_2' \cdot (r_2'' \cdot (r_2 \otimes m)) &= r_2' \cdot ((r_2'' \cdot r_2) \otimes m) \\ &= (r_2' \cdot (r_2'' \cdot r_2)) \otimes m \\ &= ((r_2' \cdot r_2'') \cdot r_2) \otimes m \\ &= (r_2' \cdot r_2'') \cdot (r_2 \otimes m), \end{aligned}$$

as required.

4.1.3. *The universal property.* So we have shown that $R_2 \underset{R_1}{\otimes} M$ has a natural structure of R_2-module. By Sect. 4.1.1, we can forget the R_2 structure and restrict our attention to $R_2 \underset{R_1}{\otimes} M$ as an R_1-module. Convoluted as this may sound, the point is that, at the end of the day, the R_2-module we've written down, $R_2 \underset{R_1}{\otimes} M$, will be precisely the "extension" mentioned before. Namely, in the world of R_2-modules, to map out of this tensor product guy to some other R_2-module N will be exactly equivalent to mapping out of M and landing in the restriction of N in the world of R_1-modules.

For example, to give an $\mathbb{R}$-linear map $\mathbb{R}^2 \to \mathbb{C}^5$ it suffices to write down where the basis elements go. But then it immediately extends uniquely to a $\mathbb{C}$-linear map $\mathbb{C}^2 \to \mathbb{C}^5$, just because we already know how to multiply by i in the target. And, of course, the inclusion $\mathbb{R}^2 \to \mathbb{C}^2$ as $\mathbb{R}$-modules (also known as $\mathbb{R}$-vector spaces) gives us a map $\mathbb{R}^2 \to \mathbb{C}^5$ out of any map $\mathbb{C}^2 \to \mathbb{C}^5$.

However, the reason we don't talk about the reverse — mapping into this tensor product — is that a $\mathbb{C}$-linear map $\mathbb{C}^5 \to \mathbb{C}^2$ may or may not land in $\mathbb{R}^2$ (it will if and only if it is the zero map, actually), so we can't just take a $\mathbb{C}$-linear map $\mathbb{C}^5 \to \mathbb{C}^2$ and produce an $\mathbb{R}$-linear map $\mathbb{C}^5 \to \mathbb{R}^2$ with such ease. (Alternatively, but equivalently, there is always a natural R_1-module map $M \to R_2 \underset{R_1}{\otimes} M$, but not the other way around.)

So consider the (above promised) map of abelian groups

$$T_{univ} : M \to R_2 \underset{R_1}{\otimes} M, \quad m \mapsto 1 \otimes m. \tag{4.2}$$

We claim that (4.2) is in fact a map of R_1-modules. Indeed, for $r_1 \in R_1$ and $m \in M$ we have

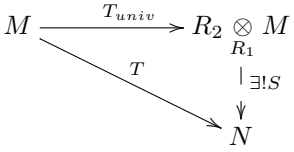
$$T_{univ}(r_1 \cdot m) = 1 \otimes (r_1 \cdot m) = (1 \cdot \phi(r_1)) \otimes m = \phi(r_1) \otimes m = r_1 \cdot (1 \otimes m) = r_1 \cdot T_{univ}(m),$$

as required.

We now claim that the map T_{univ} is universal in the following sense:

Proposition 4.1.4. *For a left R_2-module N and a map of left R_1-modules $T : M \to N$, there exists a unique map of R_2-modules $S : R_2 \underset{R_1}{\otimes} M \to N$, such that $T = S \circ T_{univ}$.*

In pictures:



We can reformulate Proposition 4.1.4 as follows:

Proposition 4.1.5. *For a left R_2-module N, precomposition with T_{univ} defines an isomorphism*

$$\mathrm{Hom}_{R_2}(R_2 \underset{R_1}{\otimes} M, N) \to \mathrm{Hom}_{R_1}(M, N). \tag{4.3}$$

It will be more convenient to prove Proposition 4.1.5:

Proof. We construct a map

$$\mathrm{Hom}_{R_1}(M, N) \to \mathrm{Hom}_{R_2}(R_2 \underset{R_1}{\otimes} M, N) \tag{4.4}$$

as follows. Given $T : M \to N$ we define $S : R_2 \underset{R_1}{\otimes} M \to N$ by

$$S(r_2 \otimes m) = r_2 \cdot T(m). \tag{4.5}$$

Week 2, Problem 1. *Show that S, specified on simple tensors by* (4.5)*, is a well-defined map of R_2-modules.*

Week 2, Problem 2. *Show that the map* (4.4) *provides an inverse to* (4.3).

□

4.1.6. *Functoriality.* Let now $T : M' \to M''$ be a map of left R_1-modules. By Lemma 2.4.4, we obtain a well-defined map of abelian groups

$$(\mathrm{id}_{R_2} \otimes T) : R_2 \underset{R_1}{\otimes} M' \to R_2 \underset{R_1}{\otimes} M''. \tag{4.6}$$

However, it is easy to see that (4.6) is in fact a map of R_2-modules (check this on the the simple tensors).

4.1.7. *An example: tensoring up vector spaces.* Back to your favorite example. Let V be a real vector space and $T : V \to V$ a linear map. If $V = \mathbb{R}^2$ and T is given by the matrix

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

we are going to be hard-pressed to find eigenvectors of T (since, of course, there are none over $\mathbb{R}^2$). But of course $e^1 \pm ie^2$ are perfectly good eigenvectors (with eigenvalues $\mp i$) in $\mathbb{C}^2$. So we just say "regard T as a matrix with complex entries. Here are its eigenvectors." What are we actually doing?

What we're doing is (no surprise) the following. We are taking $R_1 = \mathbb{R}$ and $R_2 = \mathbb{C}$, and setting

$$V_{\mathbb{C}} := \mathbb{C} \underset{\mathbb{R}}{\otimes} V; \quad T_{\mathbb{C}} := \mathrm{id}_{\mathbb{C}} \otimes T.$$

$T_{\mathbb{C}}$ is the result of "regarding" T as a complex-linear transformation.

We call $V_{\mathbb{C}}$ (resp., $T_{\mathbb{C}}$) the *complexification* of V (resp., T). By definition, *complex* eigenvectors of T are those of $T_{\mathbb{C}}$.

Week 2, Problem 3. *Show that if*

$$e_1, \ldots, e_n \tag{4.7}$$

is a basis of V, then

$$1 \otimes e_1, \ldots, 1 \otimes e_n \tag{4.8}$$

is a basis of $V_{\mathbb{C}}$ as a complex vector space. Show that if T is given, in the basis (4.7)*, by a matrix M, then $T_{\mathbb{C}}$ is given, in the basis* (4.8)*, by the* same *matrix M, viewed as having complex entries.*

4.2. **Tensor products over commutative rings.** In this subsection our ring R will be assumed commutative. Note that in this case right modules are the same as left modules (the point is that, for a right-module structure, denoting the action map by $r, m \mapsto (r, m)$ for extra clarity, $(r', (r, m)) = ((r \cdot r'), m)$, but by commutativity this is $((r \cdot' r), m)$, so the action *also* satisfies the axioms of a left module structure), so we will not distinguish between the two notions. Just for psychological ease, we'll denote the action map on the left:

$$r, m \mapsto r \cdot m.$$

4.2.1. Let M and N be two R-modules. Consider the abelian group

$$M \underset{R}{\otimes} N.$$

Originally we might have hoped that $M \underset{R}{\otimes} N$ was also an R-module, but it wasn't: the R-module structure gets "eaten up" by the tensor product relations. But in the case that R is commutative, we are in good shape, and $M \underset{R}{\otimes} N$ can be equipped with a natural R-module structure.

Namely, we define:

$$r \cdot (m \otimes n) := (r \cdot m) \otimes n. \tag{4.9}$$

Note that $(r \cdot m) \otimes n = m \otimes (r \cdot n)$, by the relations inside $M \underset{R}{\otimes} N$.

Week 2, Problem 4. *Show that* (4.9) *indeed defines an R-module structure on the abelian group $M \underset{R}{\otimes} N$. Explicitly note where you use commutativity. Further, (though the punchline has already been given away) try to equip $M \underset{R}{\otimes} N$ with an R-module structure in the not-necessarily-commutative case, and see where you hit a wall.*

Week 2, Problem 5. *Show that the switching map $m \otimes n \to n \otimes m$ defines an isomorphism of R-modules*

$$M \underset{R}{\otimes} N \to N \underset{R}{\otimes} M. \tag{4.10}$$

4.2.2. *Universal property in the commutative context.* Let P be another R-module. We define a *new* notion of R-bilinear pairing on $M \times N$ with values in P. Namely, such a thing will be defined to be a map

$$B : M \times N \to P,$$

satisfying the same requirements as in Sect. 2.3.3, plus the restriction that:

$$B(r \cdot m, n) = B(m, r \cdot n) = r \cdot B(m, n)$$

(where the last equality now makes sense because P is an R-module).

This is the more familiar notion of "bilinear pairing" that we know and love from linear algebra: $\mathbb{R}^n \underset{\mathbb{R}}{\otimes} \mathbb{R}^n \to \mathbb{R}$ via $(x_i)_i \otimes (y_i)_i \mapsto \sum x_i \cdot y_i$ is, indeed, bilinear in this new sense.

By the definition of the R-module structure on $M \underset{R}{\otimes} N$, the map

$$B_{univ} : M \times N \to M \underset{R}{\otimes} N, \quad m, n \mapsto m \otimes n$$

is an R-bilinear pairing in the new sense.

Moreover, we have the following analogue of Proposition 2.3.6:

Proposition 4.2.3. *For an R-module P, the assignment $\phi \mapsto \phi \circ B_{univ}$ is a bijection between $\mathrm{Hom}_R(M \underset{R}{\otimes} N, P)$ and the set of bilinear maps (in the new sense) $B : M \times N \to P$.*

We omit the proof as it is completely analogous to that of Proposition 2.3.6.

4.2.4. *Multilinear maps.* As mentioned way back when we were first introducing tensor products, multilinear algebra is ubiquitous in mathematics. But it turns out that, by considering a k-tuple $(m_1, \ldots, m_k)$ as a bunch of pairs

$$(m_1, (m_2, \cdots (m_{k-1}, m_k) \cdots)),$$

all of multilinear algebra is reduced to the study of tensor products.

Let's make this more precise. Let now $M_1, \ldots, M_n$ be an n-tuple of R-modules, and P yet another R-module. We define the notion of R-multilinear map from $M_1 \times \cdots \times M_n$ to P to be a map of sets

$$\mu : M_1 \times \cdots \times M_n \to P,$$

which is additive in each argument separately, and for any element $(m_1, \ldots, m_n) \in M_1 \times \cdots \times M_n$ and $r \in R$ we have

$$\begin{aligned} \mu(r \cdot m_1, m_2, \ldots, m_n) = \mu(m_1, r \cdot m_2, \ldots, m_n) = \cdots = \mu(m_1, m_2, \ldots, r \cdot m_n) \\ = r \cdot \mu(m_1, \ldots, m_n). \end{aligned}$$

For example, take $n = 3$. Consider the following maps

$$\mu'_{univ} : M_1 \times M_2 \times M_3 \to (M_1 \otimes M_2) \otimes M_3, \quad m_1, m_2, m_3 \mapsto (m_1 \otimes m_2) \otimes m_3,$$

and

$$\mu''_{univ} : M_1 \times M_2 \times M_3 \to M_1 \otimes (M_2 \otimes M_3), \quad m_1, m_2, m_3 \mapsto m_1 \otimes (m_2 \otimes m_3).$$

Week 2, Problem 6. *Show that the maps μ'_{univ} and μ''_{univ} both satisfy a universal property (hence their names) as in Proposition 4.2.3 for R-multilinear maps out of $M_1 \times M_2 \times M_3$.*

Week 2, Problem 7. *Deduce that there exists a unique isomorphism*

$$(M_1 \otimes M_2) \otimes M_3 \simeq M_1 \otimes (M_2 \otimes M_3)$$

preserving the universal maps — i.e., with the property that

$$(m_1 \otimes m_2) \otimes m_3 \mapsto m_1 \otimes (m_2 \otimes m_3).$$

4.3. **Tensor products of vector spaces.** In this subsection we will specialize further to the case when R is a field, denoted k. Note that k-modules are by definition the same as k-vector spaces. We shall often omit k from the notation, and simply write $V \otimes W$ instead of $V \underset{k}{\otimes} W$.

4.3.1. Let V be a finite-dimensional vector space with a basis $e_1, \ldots, e_n$, which we can think of as defining an isomorphism $k^n \simeq V$. Let W be some other vector space. Note that by Propositions 2.4.6 and 2.4.2 we have a canonically defined isomorphism

$$V \otimes W = k^n \otimes W \simeq (k \otimes W)^{\oplus n} \simeq W^{\oplus n},$$

under which the element $e_i \otimes w \in V \otimes W$ goes over to the element

$$(0, \ldots, 0, w, 0, \ldots, 0) \in W^{\oplus n},$$

where w is placed in the i-th slot.

From this we obtain:

Corollary 4.3.2. *If $e_1, \ldots, e_n$ is a basis for V, and $f_1, \ldots, f_m$ is a basis for W, then*

$$e_i \otimes f_j \in V \otimes W, \quad i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}$$

forms a basis for $V \otimes W$.

That is to say, $k^{\oplus m} \otimes k^{\oplus n} \simeq k^{\oplus m \cdot n}$. Immediately we see that:

Corollary 4.3.3. $\dim(V \otimes W) = \dim(V) \cdot \dim(W)$.

4.3.4. Let V and W be two arbitrary vector spaces over k. Let V^* denote the dual vector space of V, i.e., $\mathrm{Hom}(V, k)$. We define the map

$$\Phi_{V,W} : V^* \otimes W \to \mathrm{Hom}(V, W) \tag{4.11}$$

by sending $\xi \otimes w \in V^* \otimes W$ to the element $T_{\xi,w} \in \mathrm{Hom}(V, W)$, defined by

$$T_{\xi,w}(v) := \xi(v) \cdot w, \quad v \in V.$$

It is easy to show (using Proposition 4.2.3) that the assignment

$$\xi \otimes w \mapsto T_{\xi,w}$$

indeed defines a k-linear map $V^* \otimes W \to \mathrm{Hom}(V, W)$.

Proposition 4.3.5. *Suppose that either V or W is finite-dimensional. Then the map* (4.11) *is an isomorphism.*

Proof. Assume first that V is finite-dimensional. First, note that if $V = V_1 \oplus V_2$, using $(V_1 \oplus V_2)^* \simeq V_1^* \oplus V_2^*$, the following diagram commutes

$$\begin{array}{ccc} (V_1 \oplus V_2)^* \otimes W & \xrightarrow{\Phi_{V_1 \oplus V_2, W}} & \mathrm{Hom}(V_1 \oplus V_2, W) \\ \sim\uparrow & & \uparrow\sim \\ (V_1^* \otimes W) \oplus (V_2^* \otimes W) & \xrightarrow{\Phi_{V_1,W} \oplus \Phi_{V_2,W}} & \mathrm{Hom}(V_1, W) \oplus \mathrm{Hom}(V_2, W). \end{array}$$

In particular, if $\Phi_{V_1,W}$ and $\Phi_{V_2,W}$ are both isomorphisms, then so is $\Phi_{V_1 \oplus V_2, W}$.

Iterating, and using the fact that V is isomorphic to k^n for some n, we reduce the assertion of the proposition to the case when $V = k$. In this case the assertion follows from the commutativity of:

$$\begin{array}{ccc} k^* \otimes W & \xrightarrow{\Phi_{k,W}} & \mathrm{Hom}(k, W) \\ \sim\uparrow & & \uparrow\sim \\ k \otimes W & \xrightarrow{\sim} & W. \end{array}$$

Week 2, Problem 8. *Finish the proof of the proposition by handling the case of W finite-dimensional.*

□

4.3.6. Let V and W be vector spaces. We have the maps

$$\Phi_{V,W} : V^* \otimes W \to \mathrm{Hom}(V, W)$$

and

$$\Phi_{W^*,V} : (W^*)^* \otimes V^* \to \mathrm{Hom}(W^*, V^*).$$

Recall also that we have a canonically defined map

$$W \to (W^*)^*, \tag{4.12}$$

as well as a map

$$\mathrm{Hom}(V, W) \to \mathrm{Hom}(W^*, V^*), \tag{4.13}$$

corresponding to passing to the dual operator (also known as the "transpose").

Week 2, Problem 9. *Show that the following diagram is commutative:*

$$\begin{array}{ccc} (W^*)^* \otimes V^* & \xrightarrow{\Phi_{W^*,V^*}} & \mathrm{Hom}(W^*, V^*) \\ {\scriptstyle ((4.12) \otimes \mathrm{id}_{V^*}) \circ (4.10)}\uparrow & & \uparrow{\scriptstyle (4.13)} \\ V^* \otimes W & \xrightarrow{\Phi_{V,W}} & \mathrm{Hom}(V, W). \end{array}$$

4.3.7. *The infinite-dimensional case (optional material).* In this subsection we will study the map $\Phi_{V,W}$ when both V and W are infinite-dimensional.

We will assume that both V and W admit (infinite) bases, denoted e_a, $a \in A$ and f_b, $b \in B$, respectively, where A and B are infinite. (Incidentally, the axiom of choice is equivalent to the assertion that any vector space V has a basis.)

Bonus problem A1, 1pt. *Show that the map $\Phi_{V,W}$ is* not *an isomorphism.*

Bonus problem A2, 1pt. *Show that the map $\Phi_{V,W}$ is injective, and that its image is contained in the subspace $\mathrm{Hom}(V,W)_f \subset \mathrm{Hom}(V,W)$ consisting of linear operators with a finite-dimensional image.*

Bonus problem A3, 1pt. *Show that the resulting map $\Phi_{V,W} : V^* \otimes W \to \mathrm{Hom}(V,W)_f$ is an isomorphism.*

4.4. **The trace map.**

4.4.1. Let V be a vector space. We define a (familiar) map

$$\mathrm{ev}_V : V^* \otimes V \to k$$

by $\mathrm{ev}_V(\xi \otimes v) := \xi(v)$. It follows from Proposition 4.2.3 that ev_V is indeed a well-defined k-linear map $V^* \otimes V \to k$.

Assume now that V is finite-dimensional. We define the trace map

$$\mathrm{Tr}_V : \mathrm{End}(V) \to k$$

to be

$$\mathrm{ev}_V \circ (\Phi_{V^*,V})^{-1},$$

where we are using the fact that $\Phi_{V^*,V}$ is an isomorphism, given by Proposition 4.3.5.

4.4.2. Let us compare this with the usual definition of trace via matrices. Let $e_1, \ldots, e_n$ be a basis for V. For $T \in \mathrm{End}(V)$, let $\mathrm{Mat}_{(e_1,\ldots,e_n)}(T)$ be the corresponding $(n \times n)$-matrix. We claim:

Proposition 4.4.3. $\mathrm{Tr}(T) = \mathrm{Tr}(\mathrm{Mat}_{(e_1,\ldots,e_n)}(T))$*, where in the right-hand side* $\mathrm{Tr}(-)$ *denotes the usual matrix trace:*

$$(a_{ij}) \mapsto \sum_i a_{ii}.$$

Proof. Both sides are additive in T, so we can assume that $\mathrm{Mat}_{(e_1,\ldots,e_n)}(T)$ has zero entries everywhere, except for entry 1 in exactly one place. Such a T is of the form

$$T_{i^*,j} := \Phi_{V,V^*}(e_i^* \otimes e_j),$$

for some i and j, where $e_1^*, \ldots, e_n^*$ denotes the basis of V^* dual to the basis $e_1, \ldots, e_n$ of V, i.e., the linear functionals given by:

$$e_i^*(e_j) = \delta_{i,j}.$$

By the definition of the usual matrix trace, we have:

$$\mathrm{Tr}(\mathrm{Mat}_{(e_1,\ldots,e_n)}(T_{i^*,j})) = \delta_{i,j}.$$

On the other hand, by definition,

$$\mathrm{Tr}(T_{i^*,j}) = \mathrm{ev}_V \circ \Phi^{-1}_{V,V^*}(T_{i^*,j}) = \mathrm{ev}_V(e_i^* \otimes e_j) = e_i^*(e_j) = \delta_{i,j}.$$

□

It should be noted that we could have defined the trace by choosing a basis, writing down the usual definition, and then checking that our definition didn't depend on our choice of basis. But this definition makes basis-independence completely tautological. Moreover, in mathematics it has proven to be quite profitable to write down definitions without making choices, because oftentimes checking that something is independent of a few choices turns out to be ridiculously hard.

4.4.4. *Composition via tensor products.* Let U, V and W be vector spaces. Composition defines a map of sets

$$\mathrm{Hom}(U,V)\times\mathrm{Hom}(V,W)\to\mathrm{Hom}(U,W).$$

This map is easily seen to be bilinear, so by Proposition 4.2.3 it defines a map of vector spaces

$$\mathrm{Hom}(U,V)\otimes\mathrm{Hom}(V,W)\to\mathrm{Hom}(U,W). \tag{4.14}$$

Of course if U,V and W are all finite-dimensional, we already know another way to describe e.g. $\mathrm{Hom}(U,V)$: namely, $\mathrm{Hom}(U,V)\simeq U^*\otimes V$. So immediately we are led to wonder what this composition map looks like from the point of view of these isomorphisms.

Week 2, Problem 10. *Show that the following diagram commutes:*

$$\begin{array}{ccc}
\mathrm{Hom}(U,V)\otimes\mathrm{Hom}(V,W) & \longrightarrow & \mathrm{Hom}(U,W) \\
{\scriptstyle \Phi_{U,V}\otimes\Phi_{V,W}}\uparrow & & \uparrow{\scriptstyle \Phi_{U,W}} \\
(U^*\otimes V)\otimes(V^*\otimes W) & & U^*\otimes W \\
{\scriptstyle \sim}\uparrow & & \uparrow{\scriptstyle \sim} \\
U^*\otimes(V\otimes V^*)\otimes W & \xrightarrow{\mathrm{id}\otimes\mathrm{ev}_V\otimes\mathrm{id}} & U^*\otimes k\otimes W.
\end{array}$$

5. Tuesday, February 12

5.1. **More on tensor products.**

Week 3, Problem 1. *Let V and W be finite-dimensional vector spaces. Use [Problem 10, Week 2] to give a formula-free proof of the fact that for $S\in\mathrm{Hom}(V,W)$ and $T\in\mathrm{Hom}(W,V)$, we have*

$$\mathrm{Tr}_V(T\circ S)=\mathrm{Tr}_W(S\circ T).$$

Week 3, Problem 2. *Let V be a finite-dimensional vector space with basis $e_1,\dots,e_n$. Let $e_1^*,\dots,e_n^*$ be the dual basis in V^*. Recall that the collection $e_i^*\otimes e_j$ forms a basis of $V^*\otimes V$. Recall also the isomorphism*

$$V^*\otimes V\simeq\mathrm{End}(V).$$

Write the element of $V^*\otimes V$ corresponding to $\mathrm{Id}_V\in\mathrm{End}(V)$ in the basis $e_i^*\otimes e_j$.

5.1.1. Let V and W be vector spaces. Consider the set

$$\mathrm{Bil}(V\times W,k)$$

of bilinear maps (in the sense of Sect. 4.2.2). This set has a vector space structure under

$$(B_1+B_2)(v,w):=B_1(v,w)+B_2(v,w)\text{ and }(a\cdot B)(v,w):=a\cdot B(v,w).$$

Note that the isomorphism of sets between $(V\otimes W)^*:=\mathrm{Hom}(V\otimes W,k)$ and $\mathrm{Bil}(V\times W,k)$ of Proposition 4.2.3 respects the vector space structure. Hence,

Corollary 5.1.2. *There is a canonical isomorphism of vector spaces $(V\otimes W)^*\simeq\mathrm{Bil}(V\times W,k)$.*

Note that, when V and W are finite-dimensional, so is $V \otimes W$. Since for finite-dimensional vector spaces the double dual is isomorphic to the original vector space, we obtain:

Corollary 5.1.3. *For V and W finite-dimensional, there is a canonical isomorphism of vector spaces*

$$V \otimes W \simeq (\mathrm{Bil}(V \times W, k))^*.$$

Corollary 5.1.3 is the "lazy" definition of tensor product.

5.1.4. Again let V and W be arbitrary vector spaces.

Proposition 5.1.5. *There is a canonical isomorphism of vector spaces*

$$(V \otimes W)^* \simeq \mathrm{Hom}(V, W^*). \tag{5.1}$$

Proof. We construct a map forward (i.e., to the right) in (5.1) as follows. Given an element of $(V \otimes W)^*$, thought of as a bilinear pairing $B : V \times W \to k$, send it to the map $T : V \to W$ that sends $v \in V$ to the element $\xi \in W^*$, defined by

$$\xi(w) := B(v, w), \quad w \in W.$$

[Check that ξ is indeed a linear functional, that the map $V \mapsto \xi$ is linear, and that the resulting map $B \mapsto T$ is linear!]

We construct a map backwards in (5.1) as follows. Given an element $T \in \mathrm{Hom}(V, W^*)$, send it to the element of $(V \otimes W)^*$, thought of as a bilinear map $B : V \times W \to k$, defined by

$$B(v, w) := (T(v))(w).$$

[Check that B is indeed a bilinear pairing and that the assignment $T \mapsto B$ is linear.]

Week 3, Problem 3. *Check that the above maps are mutually inverse.*

□

Note that combining Proposition 5.1.5 with Corollary 5.1.3 we obtain:

Corollary 5.1.6. *The datum of a bilinear pairing $V \times W \to k$ is equivalent to the datum of a map $V \to W^*$.*

5.1.7. Let now V be an arbitrary vector space and W be finite-dimensional. On the one hand, by Proposition 4.3.5, we have a canonical isomorphism

$$W^* \otimes V \simeq \mathrm{Hom}(W, V).$$

On the other hand, by Proposition 5.1.5, and using the fact that $(W^*)^* \simeq W$ we obtain a canonical isomorphism

$$(W^* \otimes V)^* \simeq (V \otimes W^*)^* \simeq \mathrm{Hom}(V, (W^*)^*) \simeq \mathrm{Hom}(V, W).$$

Hence, we deduce a canonical isomorphism

$$(\mathrm{Hom}(W, V))^* \simeq \mathrm{Hom}(V, W). \tag{5.2}$$

Now, by Corollary 5.1.6, the datum of the isomorphism (5.2) gives rise to a pairing

$$\mathrm{Hom}(W, V) \otimes \mathrm{Hom}(V, W) \to k. \tag{5.3}$$

Week 3, Problem 4. *Show that the pairing in* (5.3) *sends $S \in \mathrm{Hom}(W, V)$, $T \in \mathrm{Hom}(V, W)$ to $\mathrm{Tr}_W(T \circ S)$.*

5.1.8. Now take V and W to be arbitrary vector spaces. Note that we have a canonical map

$$(V \otimes W) \otimes (W^* \otimes V^*)$$

$$\simeq V \otimes (W \otimes W^*) \otimes V^* \xrightarrow{\mathrm{Id}_V \otimes \mathrm{ev}_W \otimes \mathrm{Id}_{V^*}} V \otimes k \otimes V^* \simeq V \otimes V^* \xrightarrow{\mathrm{ev}_V} k. \tag{5.4}$$

By Corollary 5.1.6, the map (5.4) defines a map

$$(W^* \otimes V^*) \to (V \otimes W)^*. \tag{5.5}$$

Week 3, Problem 5. *Show that the map* (5.5) *is an isomorphism if at least one of the vector spaces V or W is finite-dimensional.*

5.2. **Groups acting on sets.**

5.2.1. Let G be a group. An action of G on a set X is a map

$$G \times X \to X, \quad (g, x) \mapsto g \cdot x$$

that satisfies:

- For any $x \in X$, we have $1 \cdot x = x$;
- For any $g_1, g_2 \in X$ and $x \in X$ we have $g_1 \cdot (g_2 \cdot x) = (g_1 \cdot g_2) \cdot x$.

Terminology: If G acts on X we shall also say that X is a G-set.

We have:

Lemma 5.2.2. *Let X be a G-set. Then for any $g \in G$ the map $x \mapsto g \cdot x$ is an automorphism of X.*

Proof. The inverse map is given by $x \mapsto g^{-1} \cdot x$. □

5.2.3. By the the lemma, from a group action we obtain a set map $G \to \mathrm{Aut}(X)$, the group of all set automorphisms of X, via $g \mapsto g\cdot$, the automorphism of X corresponding to acting by g. Our two bulleted requirements are precisely equivalent to the statement that $G \to \mathrm{Aut}(X)$ is a *homomorphism* of groups.

Conversely, given a map $\phi : G \to \mathrm{Aut}(X)$, one obtains an action via $(g, x) \mapsto \phi(g)(x)$. One checks easily that these two processes are inverse, hence the datum of a group action is exactly equivalent to the datum of a map (of groups) $G \to \mathrm{Aut}(X)$.

5.2.4. Let X_1 and X_2 be two G-sets. A map of G-sets from X_1 to X_2 is a map of sets $\phi : X_1 \to X_2$ that makes the diagram

$$\begin{array}{ccc} G \times X_1 & \longrightarrow & X_1 \\ {\scriptstyle \mathrm{id}_G \times \phi}\downarrow & & \downarrow{\scriptstyle \phi} \\ G \times X_2 & \longrightarrow & X_2 \end{array}$$

commute.

In other words, for every $x_1 \in X_1$ and $g \in G$, we have

$$g \cdot \phi(x_1) = \phi(g \cdot x_1).$$

We denote the set of maps of G-sets from X_1 to X_2 by $\mathrm{Hom}_G(X_1, X_2)$.

5.2.5. If G acts on X, we define

$$X^G = \{x \in X \,|\, \forall g \in G,\, g \cdot x = x\}.$$

We call X^G the set of G-invariants.

5.2.6. *Examples.*

(0) The empty set $\emptyset$ carries a unique action of G.

(i) For any group G, the one-element set $\{*\} =: \mathrm{pt}$ carries a unique G-action.

For any G-set X consider the map

$$\mathrm{Hom}_G(\{*\}, X) \to X$$

that sends $\phi : \{*\} \to X$ to $\phi(*) \in X$.

Lemma 5.2.7. *There is a canonical bijection of sets* $\mathrm{Hom}_G(\mathrm{pt}, X) \simeq X^G$.

Proof. To $\phi : \mathrm{pt} \to X$ we attach the element $x = \phi(*)$. It follows from the definitions that x is G-invariant. Vice versa, to $x \in X^G$ we attach the map $\phi : \mathrm{pt} \to X$ that sends $*$ to x. □

(ii) For any group G, the set $X = G$ carries a canonical G-action given by *left multiplication*. We call this G-set the *left-regular G-action*.

(iii) For any group G, the set $X = G$ carries a canonical G-action given by *right multiplication by the inverse element*

$$g \underset{\mathrm{act}}{\cdot} g' = g' \cdot g^{-1}.$$

We call this G-set the *right-regular G-action*. (Check that the naive definition without an inverse wouldn't actually define an action, and that the definition with this inverse actually does work. Hint: the point is that G may not be commutative.)

(iv) Combining Examples (ii) and (iii) we have an action of the group $G \times G$ on the set $X = G$ by

$$(g_1, g_2) \underset{\mathrm{act}}{\cdot} g' = g_1 \cdot g' \cdot g_2^{-1}.$$

(v) If G acts on X and $\phi : H \to G$ is a group homomorphism, we obtain an H action on X by composition.

(vi) We define the *adjoint* action of G on itself by

$$g \underset{\mathrm{act}}{\cdot} g' = g \cdot g' \cdot g^{-1}.$$

(vii) Let X be a set. Consider the group $G := \mathrm{Aut}_{\mathrm{Sets}}(X)$. We obtain a tautological action of G on x by

$$g \cdot x := g(x).$$

(viii) In the previous example, set $X := \{1, \ldots, n\}$. We define the symmetric group S_n to be $\mathrm{Aut}_{\mathrm{Sets}}(\{1, \ldots, n\})$. Thus, we obtain the tautological S_n-action on $\{1, \ldots, n\}$.

(ix) Let V be a vector space over a field k. We define the group $\mathrm{GL}(V)$ to be that of all k-linear automorphisms of V. We have a tautological action of $\mathrm{GL}(V)$ on V. In fact, this is a combination of Examples (v) and (vii) since $\mathrm{GL}(V)$ is a subgroup of $\mathrm{Aut}_{\mathrm{Sets}}(V)$.

(x) Let V be a complex vector space equipped with an inner form (i.e., a positive-definite Hermitian bilinear form) $(\cdot, \cdot)$. We define $\mathrm{U}(V)$ to be the subgroup of $\mathrm{GL}(V)$ consisting of those $T : V \to V$ for which $(T(v_1), T(v_2)) = (v_1, v_2)$. We call

$\mathrm{U}(V)$ the *unitary* group of V. From examples (v) and (ix) we obtain an action of $\mathrm{U}(V)$ on V.

The same works for real vector spaces with a nondegenerate symmetric bilinear form; the corresponding subgroup of $\mathrm{GL}(V)$ is denoted $\mathrm{O}(V)$ and is called the *orthogonal group of* V. (For example, the group of Lorentz transformations encountered in special relativity preserve the nondegenerate (but not positive definite!) form $\langle (t,x,y,z),(t',x',y',z')\rangle := tt' - xx' - yy' - zz'$. Hence they form a subgroup of the orthogonal group of $\mathbb{R}^4$ equipped with this form. Depending on conventions, this whole group might be called the Lorentz group. In any case the group of transformations preserving this form is often notated $\mathrm{O}(1,3)$.)

5.2.8. *Action on sets of cosets.* Let G be a group, and $H \subset G$ a subgroup. Recall that we introduced the set G/H of *right cosets* of G with respect to H. It was characterized by the property that we have a surjective map

$$\pi : G \to G/H$$

such that $\pi(g_1) = \pi(g_2)$ if and only if $g_1 = g_2 \cdot h$ with $h \in H$.

5.2.9. We now claim:

Proposition 5.2.10. *There exists a uniquely defined action of G on G/H such that π is a map of G-sets, where G acts on G by the left regular action.*

Proof. For $x \in G/H$ let $g \in G$ be such that $\pi(g) = x$. Hence, for $g_1 \in G$ we must have

$$g_1 \cdot x = g_1 \cdot \pi(g) = \pi(g_1 \cdot g).$$

This shows the uniqueness of the action. To prove the existence, we need to show that if $\pi(g') = \pi(g'')$, then $\pi(g_1 \cdot g') = \pi(g_1 \cdot g'')$. However,

$$\pi(g') = \pi(g'') \Leftrightarrow \exists h \in H \text{ s.t. } g' = g'' \cdot h.$$

Hence,

$$g_1 \cdot g' = g_1 \cdot g'' \cdot h,$$

and hence $\pi(g_1 \cdot g') = \pi(g_1 \cdot g'')$ as required.

The fact that the resulting operation $g_1, x \mapsto g_1 \cdot x$ is associative follows from the corresponding fact for G.

□

For a G-set X consider the map

$$\mathrm{Hom}_G(G/H, X) \to X \tag{5.6}$$

that sends $T : G/H \to X$ to the element $T(\pi(1))$.

Proposition 5.2.11. *The image of the map* (5.6) *belongs to the subset X^H, and the resulting map*

$$\mathrm{Hom}_G(G/H, X) \to X^H$$

is bijective. The inverse map sends $x \in X^H$ to the map ϕ uniquely characterized by the property that

$$\phi \circ \pi(g) = g \cdot x.$$

Proof. Do it yourself!

□

5.3. **Group representations.** Again let G be a group. We fix a field k and consider vector spaces over k.

5.3.1. A representation of G is a pair $\pi := (V, \phi)$, where V is a k-vector space, and ϕ denotes an action of G on V *as a vector space*. I.e., V is a G-set, such that for every $g \in G$, the map

$$v \mapsto g \cdot v$$

is k-linear.

5.3.2. As when working with G-sets, the datum of a G representation is equivalent to the datum of a map $G \to \mathrm{GL}(V)$, where now we take *linear* automorphisms rather than set automorphisms, in light of our richer structure. Concretely, were we to choose a basis $V \cong k^n$, a G-representation would attach to each element g of the group an $n \times n$ matrix m_g, such that, first, $m_e = \mathrm{id}_{n\times n}$, the $n \times n$ identity matrix, and, second, for all g and h in the group, $m_{gh} = m_g \cdot m_h$ — that is, so that the group multiplication is carried over to ("intertwined" with) multiplication of matrices.

5.3.3. Let $\pi_1 := (V_1, \phi_1)$ and $\pi_2 := (V_2, \phi_2)$ be two G-representations. A map of G-representations $\pi_1 \to \pi_2$ is a map of G-sets $T : V_1 \to V_2$ such that T is k-linear as a map of vector spaces.

Equivalently, T is a linear map $V_1 \to V_2$ which respects the action of G, i.e., for every $v_1 \in V_1$ we have

$$g \cdot T(v_1) = T(g \cdot v_1).$$

We denote the set of maps of G-representations $\pi_1 \to \pi_2$ by

$$\mathrm{Hom}_G(\pi_1, \pi_2).$$

It is easy to see that $\mathrm{Hom}_G(\pi_1, \pi_2)$ is a vector space under the operation of addition and multiplication by scalars.

5.3.4. *Examples.*

(0) The zero representation. We take the zero vector space. Any action on it is trivial.

(i) The trivial representation. We take the vector space k, and the trivial action of G. We shall denote this representation by triv_G, or just triv.

For a representation $\pi = (V, \phi)$, we let π^G be the vector space

$$\{v \in V \,|\, g \cdot v = v \text{ for all } g \in G\}.$$

We call π^G *the set of G-invariants in π*.

Lemma 5.3.5. *For a representation π there is a canonical isomorphism of vector spaces*

$$\mathrm{Hom}_G(\mathrm{triv}, \pi) \simeq \pi^G.$$

Proof. Adapt the proof of Lemma 5.2.7. □

(ii) Let G act on a set X. Take the vector space $\mathrm{Fun}(X,k)$ of *all* k-valued functions on X. We define a G-action on $\mathrm{Fun}(X,k)$ as follows: for $g \in G$ and $f \in \mathrm{Fun}(X,k)$ we define a new function $g \cdot f$ by

$$(g \cdot f)(x) = f(g^{-1} \cdot x).$$

(The inverse is there for a reason — check (very carefully!) that this does indeed define a representation, and that the definition without the inverse would not have worked. Note that this is essentially the same check as for the right action of G on itself!)

Observe that, for X finite, $\mathrm{Fun}(X,k)$ has a canonical basis as a k-vector space: $\{\delta_x\}_{x \in X}$, where $\delta_x(y) = 0$ unless $x = y$, in which case it is 1. Note that, for $g \in G$, $g \cdot \delta_x = \delta_{g \cdot x}$, which is perhaps easier to remember.

(iii) Take in the previous example $G = S_n$ and $X = \{1, \ldots, n\}$. We can identify $\mathrm{Fun}(X,k)$ with k^n. We obtain an action of S_n on k^n by "permutation of coordinates." We call this representation the *reflection representation* and denote it by refl. The reason for this name is simple: the elements of S_n are products of transpositions (i.e., permutations simply switching two points and leaving everything else fixed), and a transposition (ij) is sent to the reflection switching the i and j coordinates (i.e., through the line spanned by $e_i + e_j$, for $\{e_k\}$ the standard basis). Hence the image of an element of S_n is a product of reflections.

5.3.6. *Characters.* The word "character" is used in the context of representation theory in two different ways. This can lead to confusion. A compounding factor is that these two notions are related. Right now we will introduce one of these notions.

A character of G with values in $k^\times$ is a group homomorphism

$$\chi : G \to k^\times,$$

where $k^\times := k - \{0\}$ is a group under the multiplication inherited from the field.

To a character we assign a representation, denoted $k^\chi = (k, \chi)$. I.e., we take the vector space to be k, and $\phi : G \to \mathrm{GL}(k)$ to be given by χ, where we note that

$$\mathrm{GL}(k) = \mathrm{GL}_1(k) \simeq k^\times.$$

(Note that any representation on the vector space k is of this form: consider where $1 \in k$ is sent, and then by k-linearity you know the whole representation.)

Examples

(i) Take $k = \mathbb{C}$ and $G = \mathbb{Z}/n\mathbb{Z}$. We have a canonical homomorphism

$$\chi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$$

given by sending $\overline{k} \in \mathbb{Z}$ to $e^{\frac{2\pi i k}{n}}$ (do you see why this only depends on k mod n?).

(ii) We take k to be any field and $G = S_n$. Note that $k^\times$ always contains the subgroup $\{\pm 1\} \subset k^\times$. We define the *sign* homomorphism

$$S_n \to \{\pm 1\} \to k^\times$$

that sends $g \in S_n$ to $\mathrm{sign}(g)$, the sign of the permutation corresponding to g.

(That is to say, the map taking the value -1 for transpositions (ij), and extending by multiplicativity. It is not a priori obvious that this definition actually makes

sense (e.g. a permutation might be written as a product of an odd *and* an even number of transpositions at the same time), but it is a miracle of science that it does. Alternatively, one could take the reflection representation (but over $\mathbb{Z}$) (— which is legitimate, since the entries of the matrices are only 0 or 1 —) defined above, and compose with the determinant map: $S_n \to \mathrm{GL}_n(\mathbb{Z}) \xrightarrow{\det} \mathrm{GL}_1(\mathbb{Z}) \simeq \mathbb{Z}^\times = \{\pm 1\}$. Then the canonical map $\mathbb{Z} \to k$ for any field k gives the desired representation.)

Another way to define the sign homomorphism is to take $\mathrm{sign}(g)$ to be the parity of the number of pairs $1 \leq i < j \leq n$ such that $g(i) > g(j)$. It is easy to see that the assignment

$$g \mapsto \mathrm{sign}(g), \quad S_n \to \{\pm 1\}$$

is a group homomorphism (i.e., the product of two odd permutations is an even permutation, etc.). As an aside, the *alternating group* A_n is defined to be the kernel of this homomorphism (i.e., the subgroup of *even* permutations).

6. Thursday, Feb. 14

6.1. **Representations arising from cosets.**

6.1.1. Let X be a set acted on by G, and recall the representation $\mathrm{Fun}(X, k)$ of G, defined in Example Sect. 5.3.4(ii). We let

$$^f\mathrm{Fun}(X, k) \subset \mathrm{Fun}(X, k)$$

be the subrepresentation consisting of functions with *finite support*, i.e., those that take value 0 outside of finitely many elements of X.

6.1.2. If you find this slightly confusing, here is a more explicit description. As before, let δ_x denote the function $X \to k$ given by $x \mapsto 1$ and $y \mapsto 0$ for all $y \neq x$. The δ_x are linearly independent, and further they span $^f\mathrm{Fun}(X, k)$, as we may write any f in this space as $f = \sum_{x \in X} f(x)\delta_x$ (note that the sum is a finite sum since f is taken to have finite support!).

Recall that $g \cdot \delta_x = \delta_{gx}$. Hence, identifying δ_x with x, we may think of $^f\mathrm{Fun}(X, k)$ as (finite) formal linear combinations of elements of X — that is, expressions of the form $\sum \lambda_i x_i$ ($\lambda_i \in k, x_i \in X$), with the group G acting via $g \underset{new}{\cdot} (\sum \lambda_i x_i) = \sum \lambda_i (g \underset{old}{\cdot} x_i)$.

6.1.3. Let $H \subset G$ be a subgroup. Consider the G-set G/H and the corresponding representation $^f\mathrm{Fun}(G/H, k)$. Note that $^f\mathrm{Fun}(G/H, k)$ contains a special element, namely, $\delta_{\overline{1}}$, where $\overline{1} \in G/H$ is the coset of $1 \in G$. It is easy to see that $\delta_{\overline{1}}$ is H-invariant.

Let π be some other representation of G. We define the map

$$\mathrm{Hom}_G(^f\mathrm{Fun}(G/H, k), \pi) \to \pi^H \tag{6.1}$$

by sending $T \in \mathrm{Hom}_G(^f\mathrm{Fun}(G/H, k), \pi)$ to $T(\delta_{\overline{1}})$.

It is clear that, being a G-invariant map, T sends H-invariant elements to H-invariant elements.

We now claim:

Proposition 6.1.4. *The map* (6.1) *is an isomorphism.*

Proof. We construct the inverse map

$$\pi^H \to \mathrm{Hom}_G({}^f\mathrm{Fun}(G/H,k),\pi) \tag{6.2}$$

as follows.

Let V denote the vector space underlying π, and let $v \in V$ be an H-invariant element. We need to attach to it a G-invariant map

$$T_v : {}^f\mathrm{Fun}(G/H,k) \to V.$$

Note that the vector space ${}^f\mathrm{Fun}(G/H,k)$ admits a basis formed by elements $\delta_{\overline{g}}$ for $g \in G$. We set

$$T_v(\delta_{\overline{g}}) = g \cdot v.$$

Note that $g \cdot v$ only depends on the right coset of g mod H (i.e., gH), because v was assumed H-invariant.

Week 3, Problem 6. *Check that the map T_v defined above is indeed a map of G-representations, and that the resulting map* (6.2) *is the inverse of* (6.1).

□

6.1.5. One can view Proposition 6.1.4 as the conjunction of two independent results. Indeed, for *any* G-set X, using the second description of ${}^f\mathrm{Fun}(X,k)$ as formal linear combinations of $x \in X$, we have

$$\mathrm{Hom}_{\mathrm{Rep}(G)}({}^f\mathrm{Fun}(X,k),\pi) \simeq \mathrm{Hom}_{\mathrm{Set}(G)}(X,\pi),$$

where π is any G representation (and hence a G-set by just forgetting its vector space structure). From here, Proposition 6.1.4 tautologically follows from Proposition 5.2.11:

$$\mathrm{Hom}_{\mathrm{Rep}(G)}({}^f\mathrm{Fun}(G/H,k),\pi) \simeq \mathrm{Hom}_{\mathrm{Set}(G)}(G/H,\pi) \simeq \pi^H,$$

at least as G-sets, and then k-linearity is immediate.

6.1.6. We now consider the representation $\mathrm{Fun}(G/H,k)$. Let π be again some other representation of G.

Proposition 6.1.7. *There is a canonical isomorphism*

$$\mathrm{Hom}_G(\pi,\mathrm{Fun}(G/H,k)) \simeq \mathrm{Hom}_H(\pi,\mathrm{triv}_H).$$

Proof. Let π occur on a vector space V. We construct a map

$$\mathrm{Hom}_G(\pi,\mathrm{Fun}(G/H,k)) \to \mathrm{Hom}_H(\pi,\mathrm{triv}_H) \tag{6.3}$$

as follows.

Given a G-invariant map $T : V \to \mathrm{Fun}(G/H,k)$ we attach to it the map $\xi : V \to k$ taking $v \in V$ to the element $(T(v))(\overline{1}) \in k$. We claim that ξ is H-invariant. Indeed,

$$\xi(h \cdot v) = (T(h \cdot v))(\overline{1}) = (h \cdot T(v))(\overline{1}) =$$
$$= T(v)(h^{-1} \cdot \overline{1}) = T(v)(\overline{h^{-1}}) = T(v)(\overline{1}) = \xi(v),$$

whence invariance.

Next, we construct a map

$$\mathrm{Hom}_H(\pi,\mathrm{triv}_H) \to \mathrm{Hom}_G(\pi,\mathrm{Fun}(G/H,k)) \tag{6.4}$$

as follows.

Given an H-invariant map $\xi : V \to k$, we define the map

$$T_\xi : V \to \mathrm{Fun}(G/H, k)$$

by

$$(T_\xi(v))(\overline{g}) = \xi(g^{-1} \cdot v).$$

The fact that ξ was H-invariant implies that $\xi(g^{-1} \cdot v)$ only depends on the right coset of g mod H.

Week 3, Problem 7. *Check that the map T_ξ defined above is a map of G-representations, and that the maps* (6.3) *and* (6.4) *are mutually inverse.*

□

6.1.8. *Coinvariants.* With this we give the following definition. Let π be a representation of G, occurring on a vector space V. We define the space of G-*coinvariants* of π, denoted π_G by

$$\pi_G := V/\operatorname{Span}(g \cdot v - v,\ g \in G, v \in V).$$

Just like the invariants π^G were the largest subspace of π (i.e., V) on which G acted trivially, the coinvariants are the largest *quotient* of π (i.e., V) on which G acts trivially (do you see why?).

Week 3, Problem 8. *Construct a canonical isomorphism*

$$\mathrm{Hom}_G(\pi, \mathrm{triv}) \simeq \mathrm{Hom}_{\mathrm{Vect}}(\pi_G, k).$$

6.2. **Induced representations.**

6.2.1. Let H be a subgroup of G. We denote by Res^G_H the operation of taking a G-representation and viewing it as an H-representation. I.e., we take the same vector space, and only remember the action of elements of H.

We are now going to discuss an operation in the opposite direction. I.e., we will start with an H-representation ρ and will try to produce from it a representation of G. In fact, there will be two such constructions, denoted $\mathrm{Ind}^G_H(\rho)$ (called *induction*) and ${}^f\mathrm{Ind}^G_H(\rho)$ (or $\mathrm{ind}^G_H(\rho)$, called *finite induction*, or *compact induction*), respectively, the latter being analogous to the construction

$$M \mapsto R_2 \underset{R_1}{\otimes} M,$$

discussed in Sect. 4.1.

6.2.2. Let ρ occur on the vector space V. We define the vector space $\mathrm{Ind}^G_H(\rho)$ to consist of functions

$$f : G \to V$$

that satisfy

$$f(g \cdot h) = h^{-1} \cdot f(g), \quad \forall\, g \in G, h \in H. \tag{6.5}$$

We define the action of G on $\mathrm{Ind}^G_H(\rho)$ by

$$(g_1 \cdot f)(g) := f(g_1^{-1} \cdot g).$$

It is easy to see that if f satisfies (6.5), then so does $g_1 \cdot f$.

6.2.3. Let us analyze what $\mathrm{Ind}_H^G(\rho)$ looks like a mere vector space (ignoring the G-action). We claim that there is a (non-canonical) isomorphism

$$\mathrm{Ind}_H^G(\rho) \cong V^{\times(G/H)},$$

where the right-hand side is the direct *product* of copies of V, indexed by the set G/H.

Namely, for each element $x \in G/H$ choose $g_x \in G$ such that $\overline{g_x} = x$. Then the datum of a function $f : G \to V$ satisfying (6.5) is equivalent to the datum of an assignment taking every $x \in G/H$ to an element $f(g_x) \in V$.

Indeed, for any $g \in G$ there exists a unique $x \in G/H$ and an element h such that $g = g_x \cdot h$, and the value of f at g is recovered by

$$f(g) = h^{-1} \cdot f(g_x).$$

6.2.4. In particular, we obtain that, for any $f \in \mathrm{Ind}_H^G(\rho)$ and any given right coset of G mod H, either f vanishes on every single element of this coset, or it doesn't vanish on any element of this coset at all.

Finally, we let

$$^f\mathrm{Ind}_H^G(\rho) \subset \mathrm{Ind}_H^G(\rho)$$

be the subspace of functions that vanish outside a finite number of cosets. It is easy to see that this is a G-subrepresentation.

6.2.5. Note that the representations $^f\mathrm{Fun}(G/H, k)$ and $\mathrm{Fun}(G/H, k)$ studied in Sect. 6.1 are particular cases of $^f\mathrm{Ind}_H^G(\rho)$ and $\mathrm{Ind}_H^G(\rho)$, respectively, for $\rho = \mathrm{triv}_H$.

6.2.6. *The universal property of the finite induction.* Consider the H-representation

$$\mathrm{Res}_H^G(^f\mathrm{Ind}_H^G(\rho)).$$

We claim that there is a canonical map of H-representations

$$T_{univ} : \rho \to \mathrm{Res}_H^G(^f\mathrm{Ind}_H^G(\rho)).$$

Namely, we let ρ occur on the vector space V. We let T_{univ} send $v \in V$ to the function $f_v : G \to V$ defined by the following rule:

$$\begin{cases} \text{If } g = h \in H \text{ then } f(h) = h^{-1} \cdot v; \\ \text{If } g \notin H \text{then } f(g) = 0. \end{cases}$$

That is to say, $f_v(g) = 0$ unless $g \in H$, in which case it makes sense to act on v (since the representation has been restricted), and we are then forced to take $f_v(g) = g^{-1} \cdot v = g^{-1} \cdot f_v(1)$ (so that it is an element of the induction).

It is easy to see that f_v is indeed an element of $^f\mathrm{Ind}_H^G(\rho)$ (it is supported on exactly one coset!). Let us check that T_{univ} is a map of H-representations. k-linearity is left as an (easy) exercise. Let's check that

$$f_{h \cdot v} = h \cdot f_v$$

for all $h \in H$ and $v \in V$.

Both sides vanish on any element which is not in H. Hence, it is enough to check that they take the same value on $g = 1$ (do you see why?). But

$$f_{h \cdot v}(1) = h \cdot v \text{ and } (h \cdot f_v)(1) = f_v(h^{-1} \cdot 1) = f_v(h^{-1}) = h \cdot v,$$

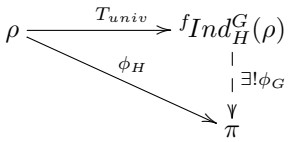
as desired.

6.2.7. Let π be a G-representation. We claim:

Proposition 6.2.8. *Precomposition with T_{univ} defines a bijection*

$$\mathrm{Hom}_G({}^f\mathrm{Ind}_H^G(\rho), \pi) \to \mathrm{Hom}_H(\rho, \mathrm{Res}_H^G(\pi)).$$

In pictures and words:



Any map of H-representations $\phi_H : \rho \to \pi$ factors as $\phi_G \circ T_{univ}$, for a unique map of G-representations $\phi_G : {}^f\mathrm{Ind}_H^G(\rho) \to \pi$.

Note the similarity of Proposition 6.2.8 with Proposition 4.1.5.

Note also that Proposition 6.1.4 is a particular case of Proposition 6.2.8 for $\rho = \mathrm{triv}_H$.

Week 3, Problem 9. *Prove Proposition 6.2.8.*

6.2.9. *The universal property of induction.* Consider now the H-representation

$$\mathrm{Res}_H^G(\mathrm{Ind}_H^G(\rho)).$$

We claim that there is a canonical map

$$T_{univ} : \mathrm{Res}_H^G(\mathrm{Ind}_H^G(\rho)) \to \rho.$$

Namely, T_{univ} sends an element $f \in \mathrm{Ind}_H^G(\rho)$ to $f(1) \in V$. We claim that T_{univ} is indeed a map of H-representations. But

$$T_{univ}(h \cdot f) = (h \cdot f)(1) = f(h^{-1}) = h \cdot f(1) = h \cdot T_{univ}(f),$$

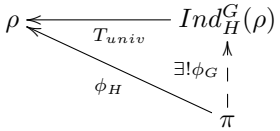
as desired.

6.2.10. Again, let π be a G-representation. We claim:

Proposition 6.2.11. *Composition with T_{univ} defines a bijection*

$$\mathrm{Hom}_G(\pi, \mathrm{Ind}_H^G(\rho)) \to \mathrm{Hom}_H(\mathrm{Res}_H^G(\pi), \rho).$$

In pictures and words:



Any map of H-representations $\phi_H : \pi \to \rho$, it factors as $T_{univ} \circ \phi_G$, for a unique map of G-representations $\phi_G : \pi \to \mathrm{Ind}_H^G(\rho)$.

Note that that Proposition 6.1.7 is a particular case of Proposition 6.2.11 for $\rho = \mathrm{triv}_H$.

Week 3, Problem 10. *Prove Proposition 6.2.11.*

These universal properties (for compact induction and induction) are generally called *Frobenius reciprocity*.

7. Tuesday, Feb. 19

7.1. The group algebra.

7.1.1. Let G be a group. It turns out that representations of G on vector spaces can be interpreted as modules over a specific ring, called the *group ring* of G. Let's get to defining this guy, who we will call $k[G]$, then.

As a vector space, $k[G]$ is the space of finite linear combinations of elements of G with coefficients in k: i.e., symbols of shape

$$\sum_{g\in G} a_g[g], \quad a_g \in k,$$

with all but finitely many $a_g = 0$.

7.1.2. We called the thing the group *ring*, so there should probably be a multiplication somewhere. In fact it is the evident one: certainly $[g]\cdot[h]$ should be $[gh]$ — so we define $[g]\cdot[h] := [gh]$. Moreover, the multiplication should distribute over addition, so we simply extend it by linearity. That is to say,

$$\left(\sum_{g\in G} a_g[g]\right)\cdot\left(\sum_{g\in G} b_g[g]\right) := \sum_{g\in G}\sum_{g'\in G} a_g\cdot b_{g'}[g\cdot g']. \tag{7.1}$$

The unit in this ring is $1[1]$, where the first 1 is the element $1\in k$ and the second 1 is the element $1\in G$ (of course we'll just write this as $[1]$). We leave checking that the proposed multiplication gives the structure of a ring as an (easy!) exercise.

We have a canonical ring homomorphism $k\to k[G]$, namely, $a\mapsto a[1]$. Note that for any $r\in k[G]$ we have

$$r\cdot a[1] = a[1]\cdot r.$$

7.1.3. *Digression.* For future reference we give the following definition:

Definition 7.1.4. *Let k be a field. A k-algebra is a ring R, equipped with a ring homomorphism $\iota : k\to R$, such that*

$$\iota(a)\cdot r = r\cdot\iota(a), \quad \forall a\in k, r\in R.$$

A homomorphism from a k-algebra R_1 to a k-algebra R_2 is a ring homomorphism $\phi : R_1\to R_2$ such that $\phi\circ\iota_1 = \iota_2$.

For example, we obtain that $k[G]$ is k-algebra. Other examples of k-algebras are $k[t]$ (and more generally $k[t_1,\dots,t_n]$), $\mathrm{Mat}_k(n\times n)$, or any extension of fields like $\mathbb{R}\subseteq\mathbb{C}$ (so that $\mathbb{C}$ is an $\mathbb{R}$-algebra here). It is worth saying that the structure of k-algebra equips R simultaneously with a ring structure and a k-vector space via

$$a\cdot r := \iota(a)\cdot r, \quad a\in k, r\in R.$$

Note that if M is an R-module, we can precompose the action of R on M with ι and obtain a structure on M of k-vector space.

Vice versa, given a k-vector space V, we can talk about extending the action of k on it to that of R.

7.1.5. The point of introducing the group algebra $k[G]$ is the following:

Lemma 7.1.6. *For a vector space V the following two pieces of structure are equivalent:*

(a) *A structure on V of G-representation.*

(b) *Extension of the vector space structure on V to that of $k[G]$-module.*

Furthermore, under this bijection, for V_i $(i = 1, 2)$ equipped with an action of G, a linear map $S : V_1 \to V_2$ is a map of G-representations if and only if it is a map of $k[G]$-modules.

Week 4, Problem 1. *Prove Lemma 7.1.6.*

7.1.7. *Finite induction, revisited.* Let $\phi : G_1 \to G_2$ be a group homomorphism. It is easy to see that the assignment

$$[g_1] \mapsto [\phi(g_1)]$$

defines a homomorphism of k-algebras $k[G_1] \to k[G_2]$.

Let now G be a group and $H \subset G$ a subgroup. Let ρ be an H-representation. On the one hand, we can consider the G-representation ${}^f\mathrm{Ind}_H^G(\rho)$. On the other hand, we can consider the $k[G]$-module

$$k[G] \underset{k[H]}{\otimes} V,$$

where V is the vector space on which ρ occurs, regarded as a $k[H]$-module. As in the general setup of $R_1 \to R_2$ from before, we regard $k[G]$ as a *right* $k[H]$ module via multiplication on the right (just so we can make sense of the tensor product!). By Lemma 7.1.6, we can regard $k[G] \underset{k[H]}{\otimes} V$ as a G-representation: $g \in G$ acts on $f \otimes v$ by sending it to $(g \cdot f) \otimes v$. It is essential here that multiplication on the *left* commutes with multiplication on the *right*.

Week 4, Problem 2. *Construct a canonical isomorphism of G-representations*

$$k[G] \underset{k[H]}{\otimes} V \simeq {}^f\mathrm{Ind}_H^G(\rho).$$

Suggested strategy: use the fact that both representations satisfy the same universal property.

7.1.8. The interpretation of G-representations as modules over a particular ring allows us to import all the notions from the general theory of R-modules to the realm of representations.

So, for instance, we automatically have the notion of direct sum and product of representations (along with their universal properties of mapping in and mapping out).

In addition, we have the notion of subrepresentation, quotient representation, and the universal property of quotient representations.

For morphisms (here, maps of G-representations), we import the notions of injection, surjection, and isomorphism of representations.

7.1.9. *Subrepresentations.* Let π be a G-representation occurring on a vector space V.

It is easy to see that subrepresentations $\pi' \subseteq \pi$ are in bijection with subspaces $V' \subseteq V$ that are G-invariant.

Here are some examples of subrepresentations.

Let G act on a set X. Consider the representation $\mathrm{Fun}(X,k)$. We define

$$\mathrm{Fun}(X,k)_{\mathrm{const}} \subseteq \mathrm{Fun}(X,k)$$

to correspond to the vector subspace that consists of *constant* functions. I.e.,

$$\mathrm{Fun}(X,k)_{\mathrm{const}} = \{f \in \mathrm{Fun}(X,k) \,|\, f(x_1) = f(x_2) \text{ for all } x_1, x_2 \in X\}.$$

It is easy to see that the subspace $\mathrm{Fun}(X,k)_{\mathrm{const}}$ is G-invariant, so it constitutes a subrepresentation of $\mathrm{Fun}(X,k)$. Furthermore, we have

$$\mathrm{Fun}(X,k)_{\mathrm{const}} \simeq \mathrm{triv}_G\,.$$

(The isomorphism in question is defined by sending $a \in k$ to the constant function with value a.)

Consider now the representation ${}^f\mathrm{Fun}(X,k)$. We define

$${}^f\mathrm{Fun}(X,k)_0 \subset {}^f\mathrm{Fun}(X,k)$$

to correspond to the vector subspace of the those functions for which

$$\sum_{x \in X} f(x) = 0.$$

(Note that the sum makes sense because we are considering functions with finite support.)

It is easy to see that the subspace ${}^f\mathrm{Fun}(X,k)_0$ is G-invariant, so it too constitutes a subrepresentation.

Another example is the zero subrepresentation. Or the full representation as a subrepresentation of itself. Finally, imagine the invertible real numbers $\mathbb{R}^\times$ acting on $\mathbb{R}^2$ via multiplication. Any line is preserved, and hence any line in $\mathbb{R}^2$ determines a subrepresentation of this group.

7.2. **Irreducibility.**

7.2.1. Let R be a ring and M an R-module. We shall say that M is irreducible if it is nonzero and does not contain any proper nonzero ("nontrivial") submodules.

7.2.2. By Sect. 7.1.8, we automatically obtain the notion of an irreducible representation.

That is to say, a representation is irreducible if and only if the underlying vector space V does not contain any proper non-zero G-invariant subspaces.

Week 4, Problem 3. *Show that π is irreducible if and only if for every nonzero $v \in V$, the elements $g \cdot v$, $g \in G$ span V.*

Week 4, Problem 4. *Take $G = S_3$ and $X = \{1,2,3\}$, so that* $\mathrm{Fun}(X,k) = \mathrm{refl}$. *Show that the corresponding representation* refl_0 *is irreducible, provided that the characteristic of k is different from* 3.

7.2.3. Let us return to the general notion of irreducible module over a ring. We claim:

Proposition 7.2.4. *Let R be a ring and M an irreducible R-module. Then M is isomorphic to R/I, where $I \subseteq R$ is a* maximal *left ideal. Vice versa, such modules are irreducible.*

Proof. Let N be a module of the form R/I for a left ideal I. Then submodules of N are in bijection with left ideals J of R that contain I. Hence N is irreducible if and only if I is maximal.

Let now M be an irreducible R-module. Pick a nonzero element $m \in M$. Then the action of R on m defines a homomorphism of R-modules

$$T : R \to M, \quad T(r) = r \cdot m.$$

The image of this map is nonzero (it contains m). Hence, by irreducibility, its image is all of M. (That is to say, $R \cdot m \subseteq M$ is a nonzero submodule, hence all of M.) Hence,

$$M \cong R/I,$$

where $I = \ker(T)$.

□

As a corollary, we obtain:

Corollary 7.2.5.

(a) *Every irreducible $\mathbb{Z}$-module is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for a prime p.*

(b) *Let k be algebraically closed. Then every irreducible $k[t]$-module is of the form $k[t]/(t-a)$ for some $a \in k$.*

7.2.6. In a way totally analogous to Lemma 7.1.6 we prove:

Lemma 7.2.7. *For a vector space V the following two pieces of structure are equivalent:*

(a) *An endomorphism $T : V \to V$.*

(b) *Extension of the k-vector space structure on V to that of a $k[t]$-module.*

Furthermore, under this bijection, for V_i ($i = 1, 2$) equipped with endomorphisms T_i a map of $k[t]$-modules $(V_1, T_1) \to (V_2, T_2)$ is exactly a linear map $S : V_1 \to V_2$ for which $S \circ T_1 = T_2 \circ S$.

In terms of this equivalence, irreducible $k[t]$-modules correspond to the vector space k equipped with the endomorphism given by multiplication by some $a \in k$.

7.3. **Schur's lemma.**

7.3.1. Let R be a k-algebra, and let M be an R-module. The fact that all elements of R commute with multiplication by an element of k implies that we have a map

$$k \to \mathrm{End}_R(M).$$

(Namely, $r \cdot (a \cdot m) = a \cdot (r \cdot m)$ for any $r \in R, a \in k$. So multiplication by a is an R-endomorphism of M.)

Now for an absolutely fundamental theorem in representation theory, which for some reason is still called a lemma:

Theorem 7.3.2 (Schur's lemma)**.** *Assume that:*

- *k is algebraically closed;*
- *M, regarded as a vector space, is finite-dimensional;*
- *M is non-zero and irreducible as an R-module.*

Then the above map $k \to \mathrm{End}_R(M)$ is an isomorphism.

Proof. The map $k \to \mathrm{End}_R(M)$ is obviously injective (each nonzero element is invertible, after all). Let T be an element of $\mathrm{End}_R(M)$. We need to show that $T = a \cdot \mathrm{Id}_M$.

Since k is algebraically closed and since M is finite-dimensional as a k-vector space, the endomorphism T, regarded as a plain old k-linear endomorphism of M, has an eigenvalue. Call it λ. Consider the corresponding eigenspace M^λ, i.e.,

$$M^\lambda := \{m \in M \,|\, T(m) = \lambda \cdot m.\}$$

The claim is that M^λ is an R-submodule of M. Indeed, for $m \in M^\lambda$ and $r \in R$,

$$T(r \cdot m) = r \cdot T(m) = r \cdot \lambda \cdot m = \lambda \cdot (r \cdot m),$$

as required.

By assumption, $M^\lambda \neq 0$. Now, since M was assumed irreducible as an R-module, we obtain that $M^\lambda = M$. I.e.,

$$T(m) = \lambda \cdot m, \quad \forall\, m \in M,$$

as required.

□

7.3.3. This subsection was not part of the lecture:

Corollary 7.3.4. *Let k be algebraically closed and let R be a* commutative *k-algebra. Let M be a nonzero irreducible R-module that is finite-dimensional as a k-vector space. Then M is isomorphic to k as a vector space, with the action of R given by a homomorphism of k-algebras $R \to k$.*

Proof. Since R is commutative, we have a canonical homomorphism

$$R \to \mathrm{End}_R(M),$$

given by the action of R on M.

However, by Theorem 7.3.2, $\mathrm{End}_R(M) \cong k$. So the above map $R \to \mathrm{End}_R(M)$ factors through a homomorphism $\phi : R \to k$. That is, R acts on M as follows:

$$r \cdot m = \phi(r) \cdot m,$$

where $\cdot$ on the right-hand side is the action of k on M.

In particular, for any $0 \neq m$, the vector subspace $k \cdot m \subset M$ is preserved by the action of R. Since M was assumed to be irreducible, we obtain that $k \cdot m = M$. That is, scaling the vector m defines an isomorphism $k \to M$ as k-vector spaces.

Finally, by construction, the composed homomorphism $k \overset{\iota}{\to} R \overset{\phi}{\to} k$ is the identity map (check this!).

□

Week 4, Problem 5. *Deduce from Corollary 7.3.4 the following assertion: Let k be algebraically closed. Let G be an* abelian *group, and let π be an irreducible finite-dimensional G-representation. Then π is of the form k^χ for some character $\chi : G \to k^*$, see Sect. 5.3.6 for the notation.*

7.3.5. The assumption that k is algebraically closed is absolutely essential for the validity of Theorem 7.3.2. For instance, here is a counter-example for $k = \mathbb{R}$. We will actually give a counter-example to Problem 5 (for $k = \mathbb{R}$), thereby to Corollary 7.3.4, and thereby to Theorem 7.3.2 itself.

Namely, take $G = \mathbb{Z}/3\mathbb{Z}$ and π the natural representation of $\mathbb{Z}/3\mathbb{Z}$ on $\mathbb{R}^2$ by rotations. (That is, take the class of $1 \in \mathbb{Z}$ inside $\mathbb{Z}/3\mathbb{Z}$ to act by rotation by $\frac{2\pi}{3}$.) It is easy to see that π is irreducible (indeed, no line in $\mathbb{R}^2$ is invariant under the rotation by 120 degrees!).

8. Thursday, Feb. 21

8.1. Some constructions of representations.

8.1.1. Let G_1 and G_2 be two groups, and let π_1 and π_2 be representations of G_1 and G_2 (occurring on vector spaces V_1 and V_2), respectively. We define the representation $\pi_1 \otimes \pi_2$ of $G_1 \times G_2$ as follows:

As a vector space, it is $V_1 \otimes V_2$, with $(g_1, g_2) \in G_1 \times G_2$ acting on $v_1 \otimes v_2$ by $(g_1 \cdot v_1) \otimes (g_2 \cdot v_2)$ (and then the action is extended by linearity).

For anyone concerned about the well definition of this action, note it realizes:

$$V_1 \otimes V_2 \xrightarrow{m_{g_1} \otimes id} V_1 \otimes V_2 \xrightarrow{id \otimes m_{g_2}} V_1 \otimes V_2$$

where m_{g_i} is multiplication by g_i.

8.1.2. Let G_1 and G_2 and π_1 and π_2 be as above. We define the representation $\underline{\underline{\mathrm{Hom}}}(\pi_1, \pi_2)$ of $G_1 \times G_2$, occurring on the vector space $\mathrm{Hom}(V_1, V_2)$, with an element $(g_1, g_2) \in G_1 \times G_2$ acting on $T : V_1 \to V_2$ by

$$g_2 \cdot T \circ g_1^{-1}.$$

(Do you see why we needed an inverse?)

8.1.3. Let us take $G_1 = G_2 = G$. We define the G-representation

$$\underline{\mathrm{Hom}}(\pi_1, \pi_2) := \mathrm{Res}_G^{G \times G}(\underline{\underline{\mathrm{Hom}}}(\pi_1, \pi_2)),$$

where $G \to G \times G$ is the diagonal map.

We claim:

Lemma 8.1.4. *There is a canonical isomorphism of vector spaces*

$$(\underline{\mathrm{Hom}}(\pi_1, \pi_2))^G \simeq \mathrm{Hom}_G(\pi_1, \pi_2).$$

Proof. By definition, the left-hand side is the subspace of $\mathrm{Hom}(V_1, V_2)$ that consists of G-invariant elements, i.e., those $T : V_1 \to V_2$ that satisfy

$$g \circ T \circ g^{-1} = T, \quad \forall g \in G.$$

The right-hand side is the subspaces $\mathrm{Hom}(V_1, V_2)$ that consists of those elements T that satisfy

$$g \circ T = T \circ g, \quad \forall g \in G.$$

This makes the assertion of the lemma manifest. □

8.1.5. Let us take in Sect. 8.1.3 $G_1 = G$ and $G_2 = \{1\}$, $\pi_1 = \pi$ and $\pi_2 = \mathrm{triv}$. The resulting representation $\underline{\underline{\mathrm{Hom}}}(\pi, k)$ is denoted π^* and is refered to as the *dual* representation.

Explicitly, π^* occurs on the dual vector space V^* and for $\xi \in V^*$ and $g \in G$, we have

$$(g \cdot \xi)(v) = \xi(g^{-1} \cdot v). \tag{8.1}$$

8.2. **The finite regular representation.**

8.2.1. Let G be a group. We consider G as a set acted on by $G \times G$ via

$$(g_1, g_2) \cdot g = g_2 \cdot g \cdot g_1^{-1}. \tag{8.2}$$

Consider ${}^f\mathrm{Fun}(G, k)$ as a representation of $G \times G$. We denote it also by ${}^f\mathrm{Reg}(G)$, and call it the *finite regular representation*.

8.2.2. Let π_1 and π_2 be representations of G. We claim:

Proposition 8.2.3. *There is a canonical isomorphism*

$$\mathrm{Hom}_{G\times G}({}^f\mathrm{Reg}(G), \underline{\underline{\mathrm{Hom}}}(\pi_1, \pi_2)) \simeq \mathrm{Hom}_G(\pi_1, \pi_2).$$

Proof. By Lemma 8.1.4, the right-hand side is canonically isomorphic to

$$(\underline{\mathrm{Hom}}(\pi_1, \pi_2))^G.$$

We now claim that for any representation π of $G \times G$ there is a canonical isomorphism

$$\mathrm{Hom}_{G\times G}({}^f\mathrm{Reg}(G), \pi) \simeq \left(\mathrm{Res}^{G\times G}_G(\pi)\right)^G.$$

We will deduce this from Proposition 6.1.4. We apply it to the ambient group being $G \times G$ and the subgroup the diagonal copy of G. Hence, the required assertion follows from the next lemma:

Lemma 8.2.4. *There is a canonical isomorphism of sets acted on by $G \times G$:*

$$(G \times G)/G \simeq G,$$

where the $G \times G$ action on the right-hand side is given by (8.2).

Proof. We construct the map $(G \times G)/G \to G$ using Proposition 5.2.11. It corresponds to the point $1 \in G$. Namely, take $(g_1, g_2) \mapsto g_2 \cdot g_1^{-1}$. It is easy to see that this map is an isomorphism: the inverse map sends $g \in G$ to the coset of $(1, g)$. □

This completes the proof.

□

8.2.5. Take now $\pi_1 = \pi_2 = \pi$. Note that the set $\mathrm{Hom}_G(\pi, \pi)$ contains a distinguished element, namely the identity map Id_π. Applying Propositon 8.2.3, we obtain a canonically defined map of $G \times G$-representations

$$ {}^f\mathrm{Reg}(G) \to \underline{\underline{\mathrm{Hom}}}(\pi, \pi) \tag{8.3}$$

In particular, we obtain a map of vector spaces

$$ {}^f\mathrm{Fun}(G, k) \to \mathrm{Hom}(V, V). \tag{8.4}$$

But note that there is a canonical isomorphism of vector spaces

$$ {}^f\mathrm{Fun}(G, k) \simeq k[G],$$

which sends the basis element $\delta_g \in {}^f\mathrm{Fun}(G, k)$ to $[g] \in k[G]$.

Week 4, Problem 6. *Show that the map* (8.4) *corresponds to the map*

$$ k[G] \to \mathrm{End}(V),$$

given by the action of $k[G]$ on V, where we view V as a $k[G]$-module via Lemma 7.1.6.

8.3. **The regular representation.**

8.3.1. We view G as a $G \times G$-set as above. Again, set

$$ \mathrm{Reg}(G) := \mathrm{Fun}(G, k) \in \mathrm{Rep}(G \times G).$$

8.3.2. Let π_1 and π_2 be representations of G.

We claim:

Proposition 8.3.3. *There is a canonical isomorphism*

$$ \mathrm{Hom}_{G\times G}(\pi_1 \otimes \pi_2, \mathrm{Reg}(G)) \simeq \mathrm{Hom}_G(\pi_1 \otimes \pi_2, \mathrm{triv}_G),$$

where on the right-hand side we view $\pi_1 \otimes \pi_2$ as a representation of G obtained by restriction with respect to the diagonal map.

Proof. Apply Proposition 6.1.7 to the same groups as in the proof of Proposition 8.2.3.

□

8.3.4. Let us take $\pi_1 = \pi$ and $\pi_2 = \pi^*$. Note that the canonical pairing

$$ \mathrm{ev} : V \otimes V^* \to k$$

is G-invariant, where G acts on $V \otimes V^*$ diagonally (check this!). Hence it gives rise to an element of

$$ \mathrm{Hom}_G(\pi \otimes \pi^*, \mathrm{triv}_G).$$

Hence, by Proposition 8.3.3, it gives rise to a canonically defined map of $G \times G$-representations

$$ \pi \otimes \pi^* \to \mathrm{Reg}(G).$$

At the level of underlying vector spaces, we thus obtain a map

$$ V \otimes V^* \to \mathrm{Fun}(G, k). \tag{8.5}$$

Our current goal is to describe this map differently.

8.3.5. Consider the following map, denoted MC_π, and called the *matrix coefficient map*:

$$V \otimes V^* \to \mathrm{Fun}(G, k),$$

sending $v \otimes \xi \in V \otimes V^*$ to the function $\mathrm{MC}_\pi(v, \xi)$, whose value at $g \in G$ is defined to be

$$\xi(g \cdot v).$$

(Again, the map is then defined by extending by linearity.)

Week 4, Problem 7. *Show that the map* (8.5) *coincides with* MC_π.

8.4. **The character of a representation.**

8.4.1. Let π be finite-dimensional. The character of π is a function on G, denoted ch_π and defined by

$$\mathrm{ch}_\pi(g) := \mathrm{Tr}(T_g, V),$$

where T_g denotes the endomorphism of V defined by the action of $g \in G$.

8.4.2. Recall that we have an isomorphism

$$V \otimes V^* \simeq \mathrm{End}(V);$$

in particular, the element $\mathrm{Id}_V \in \mathrm{End}(V)$ defines a canonical element $u_V \in V \otimes V^*$.

Week 4, Problem 8. *Prove (without choosing bases) that* $\mathrm{MC}_\pi(u_V) = \mathrm{ch}_\pi$.

Suggested strategy: let V be a vector space, and T an endomorphism of V. Show that the following diagram commutes

$$\begin{array}{ccc} V \otimes V^* & \xrightarrow{(4.11)} & \mathrm{End}(V) \\ {\scriptstyle T \otimes \mathrm{Id}_{V^*}}\uparrow & & \uparrow{\scriptstyle S \mapsto T \circ S} \\ V \otimes V^* & \xrightarrow{(4.11)} & \mathrm{End}(V), \end{array}$$

and use this to your advantage.

8.5. **Modules of finite length.**

8.5.1. Let R be a ring, and M an R-module.

Definition 8.5.2. *We say that M is* of finite length *if it admits a finite filtration, i.e., a sequence of submodules*

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n = M$$

such that the successive quotients M_i/M_{i-1} are irreducible.

8.5.3. Let R be a field k. Then a (nonzero) vector space is irreducible as a k-module if and only if it is one-dimensional. From here, it is easy to see that a vector space has finite length if and only if it is finite-dimensional: if one admits a filtration as above, $\dim(M) = \sum \dim(M_i/M_{i-1})$ — if we know each $M_i/M_{i-1} \simeq k$, we have $\dim(M) = n$. If M is finite dimensional, choose a basis $(e_1, \dots, e_n)$, then

$$0 \subsetneq (e_1) \subsetneq (e_1, e_2) \dots \subsetneq (e_1, \dots, e_n) = M$$

is of the desired shape.

Take $R = \mathbb{Z}$. We know that all irreducible $\mathbb{Z}$-modules (i.e., abelian groups) are of the form $\mathbb{Z}/p\mathbb{Z}$. Hence any abelian group of finite length is finite: if we have $H \subseteq G$, by counting cosets (each of size $|H|$), we have $|G| = |H||G/H|$. Combining this with induction, we have $|M| = \prod_i p_i$, where $M_i/M_{i-1} \cong \mathbb{Z}/p_i\mathbb{Z}$. Vice versa:

Lemma 8.5.4. *Any finite abelian group has a finite length as a $\mathbb{Z}$-module.*

Proof. We will induct on the order of the group. Let A be a finite abelian group. Let $A' \subset A$ be a nontrivial subgroup of minimal order. It is easy to see that A' is irreducible. Set $A_1 := A'$. Now apply the induction hypothesis to $A'' := A/A'$. We obtain a filtration

$$0 = A''_0 \subsetneq A''_1 \subsetneq \dots \subsetneq A''_{n-1} \subsetneq A''_n = A''.$$

For $i \geq 1$, define A_i to be the preimage of A''_{i-1} under the natural projection $A \twoheadrightarrow A''$. Then

$$0 = A_0 \subsetneq A_1 \subsetneq \dots \subsetneq A_n \subsetneq A_{n+1} = A$$

is of the desired shape.

□

8.5.5. Let now $R = k[t]$. We know that irreducible $k[t]$-modules are all of the form $k[t]/(p(t))$, where $p(t)$ is an irreducible polynomial over k. In particular, they are all finite-dimensional as k-vector spaces. Hence, any $k[t]$-module of finite length is also finite-dimensional as a k-vector space. Vice versa:

Lemma 8.5.6. *Any $k[t]$-module which is finite-dimensional as a k-vector space is of finite length as a $k[t]$-module.*

Proof. Same idea as in the proof of Lemma 8.5.4, where, instead of the order of the abelian group, we use the dimension of the underlying k-vector space. □

9. Tuesday, Feb. 26

9.1. **Jordan-Hölder content.**

9.1.1. The following lemma will be used repeatedly (prove it!):

Lemma 9.1.2. *Let $T : M_1 \to M_2$ be a non-zero map of R-modules.*

(a) *If M_1 is irreducible, then T is injective.*

(b) *If M_2 is irreducible, then T is surjective.*

(c) *If M_1 and M_2 are irreducible, then T is an isomorphism.*

9.1.3. Let M be an R-module of finite length. Let N be an irreducible R-module. For a filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_{n-1} \subset M_n = M \tag{9.1}$$

with M_i/M_{i-1} irreducible, we define the integer $[M : N]$ as the number of indices i sich that M_i/M_{i-1} is isomorphic to N. We call this integer the *multiplicity* of N in M.

Theorem 9.1.4. *The integer $[M : N]$ is independent of the choice of the filtration.*

This is in evident analogy with the unique prime factorization of an integer (which is in fact a corollary!): when factorizing an integer k, the power of a prime p appearing in the factorization is an invariant of k.

9.1.5. Let $\mathrm{Irred}(R)$ be the set of isomorphism classes of irreducible R-modules. For each element $\alpha \in \mathrm{Irred}(R)$ we choose a representative M_α in this isomorphism class.

9.1.6. Let M be an R-module. The assignment

$$\alpha \in \mathrm{Irred}(R) \rightsquigarrow [M : M_\alpha]$$

is called the *Jordan-Hölder* content of M.

Note that the filtration (9.1) has the property that:

$$n = \sum_{\alpha \in \mathrm{Irred}(R)} [M : M_\alpha].$$

Hence, from Theorem 9.1.4, we obtain:

Corollary 9.1.7. *The integer n in (9.1) is independent of the choice of the filtration.*

The integer n in Corollary 9.1.7 is called the *length* of M and is denoted $\lg(M)$.

9.1.8. *Proof of Theorem 9.1.4.* Since we don't yet know that the length of a module is well-defined (but we'd like to induct on something), we provisionally define $\lg(M)$ as the minimum of the lengths of all possible filtrations as in (9.1).

We'll prove the theorem by induction on $\lg(M)$.

The base of the induction is $\lg(M) = 1$. In this case M is irreducible and assertion is obvious: M_1 is always necessarily all of M. So we assume that the theorem holds for all modules of length $\leq m-1$. Let M be a module of length m, and let

$$0 = M'_0 \subset M'_1 \subset \cdots \subset M'_{m-1} \subset M'_m = M$$

be a filtration of length m. Consider the module $\widetilde{M} := M/M'_1$. It admits a filtration

$$0 = \widetilde{M}'_0 \subset \widetilde{M}'_1 \subset \cdots \subset \widetilde{M}'_{m-1} \subset \widetilde{M}'_{m-1} = \widetilde{M}, \tag{9.2}$$

where $\widetilde{M}'_i = M'_{i+1}/M'_1$, $i = 0, \ldots, m-1$ (i.e. simply take the images of the M'_i under $M \to M/M'_1$).

By the third isomorphism theorem, for every $i = 0, \ldots, m-1$,

$$\widetilde{M}'_i/\widetilde{M}'_{i-1} \simeq M'_{i+1}/M'_i.$$

In particular, the filtration (9.2) has irreducible successive quotients, so $\lg(\widetilde{M}) \leq m-1$. Hence, by our induction hypothesis, the assertion of the theorem holds for

$\widetilde{M}$. That is to say, the integers $[\widetilde{M} : M_\alpha]$ are independent of our choice of filtration for $\widetilde{M}$.

Let now

$$0 = M_0 \subset M_1 \subset \cdots \subset M_{n-1} \subset M_n = M$$

be some other filtration on M. Let $\alpha_0 \in \mathrm{Irred}(R)$ be the index such that $M_1' \cong M_{\alpha_0}$. We will show that, with respect to this new filtration,

$$[M : M_\alpha] = \begin{cases} [\widetilde{M} : M_\alpha] + 1 & \text{if } \alpha = \alpha_0, \\ [\widetilde{M} : M_\alpha] & \text{if } \alpha \neq \alpha_0. \end{cases} \tag{9.3}$$

This implies the assertion of the theorem.

Let i be the minimal integer such that the submodule $M_1' \subset M$ is contained in M_i. Note that for $j < i$ the map

$$M_j \to M \to \widetilde{M} \tag{9.4}$$

is injective (indeed, otherwise we would have the kernel $M_j \cap M_1' \neq 0$, and, since M_1' is irreducible, it would follow that $M_j \cap M_1' = M_1'$, whence $M_1' \subset M_j$, contradicting the minimality of i).

We define the filtration

$$0 = \widetilde{M}_0 \subset \widetilde{M}_1 \subset \cdots \subset \widetilde{M}_{n-1} = \widetilde{M}$$

as follows.

For $j < i$, let $\widetilde{M}_j$ be the image of the map (9.4). For $j \geq i$, let $\widetilde{M}_j$ be the image of the map

$$M_{j+1} \to M \to \widetilde{M}.$$

Note that this image is isomorphic to M_{j+1}/M_1'.

We claim that the resulting filtration has irreducible successive quotients. Moreover, we claim that

$$\widetilde{M}_j/\widetilde{M}_{j-1} \simeq \begin{cases} M_j/M_{j-1} & \text{if } j < i, \\ M_{j+1}/M_j & \text{if } j \geq i. \end{cases} \tag{9.5}$$

Of course (9.5) implies (9.3), thereby proving the theorem (thanks to our inductive hypothesis).

To prove (9.5) we will consider separately the following three cases: (a) $j < i$, (b) $j > i$, and (c) $j = i$.

In case (a), there is nothing to prove, since $M_j \to \widetilde{M}_j$ and $M_{j-1} \to \widetilde{M}_{j-1}$ are isomorphisms.

Case (b) follows from the third isomorphism theorem:

$$\frac{\tilde{M}_j}{\tilde{M}_{j-1}} = \frac{M_{j+1}/M_1'}{M_j/M_1'} \simeq \frac{M_{j+1}}{M_j + M_1'} = \frac{M_{j+1}}{M_j},$$

since $M_1' \subseteq M_j$ by assumption.

Finally, in case (c) we have $\widetilde{M}_i \simeq M_{i+1}/M_1'$, and the map $\widetilde{M}_{i-1} \to \widetilde{M}_i$ identifies with the composition

$$M_{i-1} \to M_{i+1} \to M_{i+1}/M_1'.$$

That is, $\widetilde{M}_i/\widetilde{M}_{i-1}$ identifies with $M_{i+1}/(M_{i-1}+M'_1)$. Thus, it is sufficient to show that the submodule $M_{i-1}+M'_1$ of M is just M_i.

But we automatically have $M_{i-1}+M'_1 \subset M_i$, just by definition of i. For equality, it is enough to show that the map

$$M'_1 \to M_i \to M_i/M_{i-1}$$

is surjective. This map is nonzero (otherwise M'_1 would be contained in M_{i-1}). Hence it is surjective by Lemma 9.1.2.

□

9.2. **Digression: splittings of short exact sequences.**

9.2.1. Let $M_1 \to M \to M_2$ be maps of R-modules. We will say that they form a *short exact sequence* if

- $M_1 \to M$ is injective;
- $M \to M_2$ is surjective;
- The image of the former map equals the kernel of the latter.

We write a short exact sequence as

$$0 \to M_1 \to M \to M_2 \to 0.$$

We will use this notation only when the three do form a short exact sequence. Maps $A \to B \to C$ are said to be *exact* at B when the image of $A \to B$ is the kernel of $B \to C$. A short exact sequence $0 \to A \to B \to C \to 0$ is precisely a five term sequence for which every composition (e.g., $B \to C \to 0$) is exact. (Do you see why? For instance, check that to say that $B \to C \to 0$ is exact (at C) is precisely to say that $B \to C$ is a surjection, and similarly to say that $0 \to A \to B$ is exact is precisely to say that $A \to B$ is injective. Hence exactness of $0 \to A \to B \to 0$ is equivalent to $A \to B$ being an isomorphism.)

9.2.2. Let

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M & \longrightarrow & M_2 & \longrightarrow & 0 \\ & & {\scriptstyle T_1}\uparrow & & {\scriptstyle T}\uparrow & & \uparrow{\scriptstyle T_2} & & \\ 0 & \longrightarrow & M'_1 & \longrightarrow & M' & \longrightarrow & M'_2 & \longrightarrow & 0 \end{array}$$

be a commutative diagram of short exact sequences.

Week 5, Problem 1. *Assume that T_1 and T_2 are injective/surjective/bijective. Show that in this case T is also injective/surjective/bijective.*

9.2.3. Let M be an R-module and let

$$0 \to M_1 \xrightarrow{\phi} M \xrightarrow{\psi} M_2 \to 0 \tag{9.6}$$

be a short exact sequence.

We define a *splitting* of the short exact sequence to be an isomorphism of modules

$$\xi : M \to M_1 \oplus M_2$$

such that

- $\xi \circ \phi = i_1$ as maps $M_1 \to M_1 \oplus M_2$ (here i_1 is the tautological inclusion $M_1 \xrightarrow{(\mathrm{id},0)} M_1 \oplus M_2$);

- $\psi = p_2 \circ \xi$ as maps $M \to M_2$ (here p_2 is the tautological projection $M_1 \oplus M_2 \to M_2$).

That is, a map ξ making the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{\phi} & M & \xrightarrow{\psi} & M_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \xi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & M_1 & \xrightarrow{i_1} & M_1 \oplus M_2 & \xrightarrow{p_2} & M_2 & \longrightarrow & 0 \end{array}$$

commute (— this is then automatically an isomorphism by the previous lemma).

We let $\mathrm{Split}(M)$ denote the set of splittings, i.e., the set of isomorphisms ξ satisfying the above conditions.

We define a map from $\mathrm{Split}(M)$ to the set $\text{L-inv}(\phi)$ of left inverses of the map ϕ (i.e., maps $q : M \to M_1$, such that $q \circ \phi = \mathrm{id}_{M_1}$) by sending ξ to the map $p_1 \circ \xi$.

We define a map from $\mathrm{Split}(M)$ to the set of $\text{R-inv}(\psi)$ of right inverses of the map ψ (i.e., maps $j : M_2 \to M$, such that $\psi \circ j = \mathrm{id}_{M_2}$) by sending ξ to the map $\xi^{-1} \circ i_2$, where ξ^{-1} is the map inverse to ξ.

Week 5, Problem 2. *Show that the maps*

$$\text{L-inv}(\phi) \leftarrow \mathrm{Split}(M) \to \text{R-inv}(\psi),$$

defined above, are isomorphisms. (This result is called the splitting lemma*.)*

Week 5, Problem 3. *Show that the short exact sequence*

$$0 \to \mathbb{Z} \xrightarrow{2\cdot -} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

does not admit a splitting.

9.3. **Completely reducible modules.**

9.3.1. Let M be an R-module. We will say that M is *completely reducible* if it isomorphic to a finite direct sum of irreducible modules.

Note that any completely reducible module automatically has finite length.

9.3.2. *Examples.* Let R be a field k. Then any finite-dimensional vector space is completely reducible (choose a basis!).

Let R be $\mathbb{Z}$ or $k[t]$. Then it is *not* true that any finite length module is completely reducible. (For instance, $\mathbb{Z}/4\mathbb{Z}$ or $k[t]/(t^2)$.)

Let $R = k[G]$, where G is a finite group and k is a field of characteristic 0. We will show that in this case every R-module of finite length is completely reducible.

9.3.3. We will prove:

Theorem 9.3.4. *Let M be completely reducible. Then any submodule $M' \subset M$ admits a direct complement, i.e., the short exact sequence*

$$0 \to M' \to M \to M/M' \to 0$$

admits a splitting. Further, M' is itself completely reducible.

Proof. We will induct on $\lg(M)$. The base of the induction is when $\lg(M) = 1$, i.e. M is irreducible, and the assertion is clear. So, we assume that for a given M, the assertion of the theorem holds for all modules of strictly smaller length.

Write

$$M = \bigoplus_{i=1}^{n} M_i,$$

where M_i are (non-zero) irreducible modules. Set $N := \bigoplus_{i=2}^{n} M_i$, i.e.,

$$M \simeq M_1 \oplus N.$$

So now let $M' \subset M$ be a submodule as in the theorem statement. Consider the following two cases: (a) $M_1 \cap M' \neq 0$ and (b) $M_1 \cap M' = 0$.

In case (a), since M_1 is irreducible, we have $M_1 \cap M' = M_1$, i.e., $M_1 \subset M'$. In this case

$$M' \simeq M_1 \oplus N',$$

where N' is a submodule of N, namely $N \cap M'$ (e.g. because the left inverse to the inclusion $M_1 \to M$ can be restricted to M' to give a splitting of $0 \to M_1 \to M' \to M'/M_1 \to 0$). The complete reducibility of N' follows from that of N by the induction hypothesis. Moreover, N' admits a direct complement in N:

$$N \simeq N' \oplus N'',$$

again by the induction hypothesis. The same N'' provides a direct complement to $M' \simeq M_1 \oplus N'$ inside $M \simeq M_1 \oplus N$.

In case (b), the composed map

$$M' \to M \simeq M_1 \oplus N \to N,$$

denoted ψ, is injective. The complete reducibility of M' follows from that of N by the induction hypothesis. Moreover, the above map ψ admits a left inverse, again by the inductive hypothesis. Call it q (see Problem 2). The sought-for left inverse of the original map $M' \to M$ is given by the composition

$$M \simeq M_1 \oplus N \to N \xrightarrow{q} M'.$$

□

Week 5, Problem 4. *Let M be an R-module of finite length. Show that the following are equivalent: (a) M is completely reducible; (b) any submodule of M admits a direct sum complement; (c) any irreducible submodule of M admits a direct sum complement.*

10. Thursday, Feb. 28

10.1. **Tensor products of algebras and modules.**

10.1.1. Let k be an algebraically closed field, and let A_1 and A_2 be two k-algebras. We consider the vector space

$$A_1 \otimes_k A_2 =: A_1 \otimes A_2,$$

and we claim that it has a natural algebra structure. Namely, it is given by

$$(a_1' \otimes a_2') \cdot (a_1'' \otimes a_2'') = (a_1' \cdot a_1'') \otimes (a_2' \cdot a_2'').$$

The verifications of well-definition and the algebra axioms are straightforward.

Similarly, if M_1 and M_2 are modules over A_1 and A_2, respectively, the vector space

$$M_1 \otimes M_2$$

obtains a natural structure of module over $A_1 \otimes A_2$.

10.1.2. Consider the simplest example of $A_1 = A$ and $A_2 = k$, where $k \to A_2$ is the identity map. Then the algebra $A \otimes k$ is isomorphic to A.

At the level of modules we obtain the statement that, for M an A-module and V a k-vector space, the tensor product $M \otimes V$ is an A-module.

The A-module structure on $M \otimes V$ implied above is the usual one: $a \in A$ acts on $m \otimes v$ by sending it to $(a \cdot m) \otimes v$.

In particular, if $V = k^n$, we have $M \otimes k^n \simeq M^{\oplus n}$.

10.1.3. *The universal property.* Note that the k-algebra $A_1 \otimes A_2$ comes equipped with canonical homomorphisms

$$\phi_{univ,1} : A_1 \to A_1 \otimes A_2 \leftarrow A_2 : \phi_{univ,2},$$

where

$$\phi_{univ,1}(a_1) = a_1 \otimes 1 \text{ and } \phi_{univ,2}(a_2) = 1 \otimes a_2.$$

Note also that the images of $\phi_{univ,1}$ and $\phi_{univ,2}$ in $A_1 \otimes A_2$ commute:

$$(a_1 \otimes 1) \cdot (1 \otimes a_2) = (a_1 \otimes a_2) = (1 \otimes a_2) \cdot (a_1 \otimes 1).$$

Week 5, Problem 5. *Let B be a k-algebra. Show that pre-composition with $\phi_{univ,1}$ and $\phi_{univ,2}$ defines a bijection between the set of algebra homomorphisms $A_1 \otimes A_2 \to B$ and the set of pairs of algebra homomorphisms*

$$\phi_1 : A_1 \to B \leftarrow A_2 : \phi_2,$$

whose images in B commute, i.e., $\phi_1(a_1) \cdot \phi_2(a_2) = \phi_2(a_2) \cdot \phi_1(a_1)$ for every $a_1 \in A_1, a_2 \in A_2$.

10.1.4. *More examples.* Let G_1 and G_2 be groups.

Week 5, Problem 6.

(a) *Construct an isomorphism of k-algebras $k[G_1] \otimes k[G_2] \simeq k[G_1 \times G_2]$.*

(b) *Construct an isomorphism of k-algebras*

$$k[t_1, \dots, t_n] \otimes k[s_1, \dots, s_m] \simeq k[t_1, \dots, t_n, s_1, \dots, s_m].$$

Suggested strategy for point (b): show that the datum of homomorphism of k-algebras $\phi : k[t_1, \dots, t_n] \to B$ is equivalent to that of an n-tuple of elements

$$\{b_1, \dots, b_n\} \subset B, \quad b_i \cdot b_j = b_j \cdot b_i, \quad \forall i, j$$

via

$$\phi \rightsquigarrow \phi(t_1), \ldots, \phi(t_n).$$

10.2. **Burnside's theorem.** In this subsection the field k will be assumed algebraically closed. All modules will be assumed finite-dimensional over k. These assumptions allow us to apply Schur's lemma (and, indeed, we make them precisely so that we may appeal to Schur's lemma in our arguments).

10.2.1. Let A be a k-algebra, and M an A-module. For a pair of vector spaces V_1 and V_2 we have a natural map

$$\mathrm{Hom}_k(V_1, V_2) \xrightarrow{\mathrm{id} \otimes -} \mathrm{Hom}_A(M \otimes V_1, M \otimes V_2). \tag{10.1}$$

Proposition 10.2.2. *Suppose that M is irreducible. Then* (10.1) *is an isomorphism.*

Proof. Let $V_1 = V_1' \oplus V_1''$. It is easy to see that if the assertion of the proposition is true for V_1' and V_1'', then it is true for V_1. This allows us to reduce to the case when V_1 is one-dimensional, i.e., $V_1 \cong k$.

Similarly, we reduce to the case when $V_2 \cong k$. In this case, the assertion of the proposition reads as the claim that

$$k \to \mathrm{End}_A(M)$$

is an isomorphism. This is Schur's lemma. □

10.2.3. *Interlude.* Let W be a vector space and let $T : V' \to V$ be a map between finite-dimensional vector spaces. Consider the map

$$\mathrm{id}_W \otimes T : W \otimes V' \to W \otimes V.$$

Lemma 10.2.4. *If T is injective, then so is* $\mathrm{id}_W \otimes T$.

Proof. Since we are dealing with vector spaces, if a map T is injective, then it admits a left inverse (every short exact sequence of vector spaces splits: choose bases!). Call this left inverse $S : V \to V'$. But then $\mathrm{id}_W \otimes S$ provides a left inverse to $\mathrm{id}_W \otimes T$:

$$(\mathrm{id}_W \otimes S) \circ (\mathrm{id}_W \otimes T) = \mathrm{id}_W \otimes (S \circ T) = \mathrm{id}_W \otimes \mathrm{id}_V = \mathrm{id}_{W \otimes V}.$$

Finally, any map with a left inverse is automatically injective.

□

Week 5, Problem 7. *Give a counterexample to Lemma 10.2.4 over the ring $k[t]$.*

Week 5, Problem 8. *Let V and W be finite-dimensional, and let $V' \subset V$ and $W' \subset W$ be subspaces. Let us view $W \otimes V'$ and $W' \otimes V$ as subspaces of $W \otimes V$ (the corresponding maps are indeed injective by Lemma 10.2.4). Show that*

$$(W \otimes V') \cap (W' \otimes V) = W' \otimes V'.$$

10.2.5. We now claim:

Theorem 10.2.6. *Let M be an irreducible A-module, and let V be a finite-dim vector space. Then any A-submodule of $M \otimes V$ is of the form $M \otimes V'$ for a vector subspace $V' \subset V$.*

Proof. Let M' be an A-submodule of $M \otimes V$.

Choosing a basis for V, we obtain $M \otimes V \cong M^{\oplus n}$. Hence, $M \otimes V$ is a completely reducible A-module.

Hence, by Theorem 9.3.4, we obtain that M' is also completely reducible. Write

$$M' \cong \bigoplus_i M_i,$$

where M_i are irreducible. We claim that all M_i are isomorphic to M. Indeed, for any M_i, we have a non-zero map

$$M_i \to M' \to M \otimes V \cong M^{\oplus n}.$$

Hence, at least one of the components of this map is non-zero. Thus, by composing with the projection to this factor, we obtain that there exists a non-zero map $M_i \to M$. Since both M_i and M are irreducible, we obtain that the above map is an isomorphism.

Hence, we can write

$$M' \cong M^{\oplus m},$$

i.e., $M' \cong M \otimes V'$ for some other vector space V'.

The inclusion $M' \to M \otimes V$ is thus a map

$$M \otimes V' \to M \otimes V. \tag{10.2}$$

By Proposition 10.2.2, the map (10.2) comes from an inclusion $V' \to V$ (it is injective because tensoring up with M produces an injective map); identifying V' with its image in V yields the result.

□

10.2.7. From the innocuous-looking Theorem 10.2.6, we will deduce the following striking corollary:

Theorem 10.2.8. *Let M be an irreducible A-module. Let $m_1, \ldots, m_n \in M$ be vectors that are linearly independent over k. Let $m'_1, \ldots, m'_n \in M$ be an* arbitrary *n-tuple of elements. Then there exists an element $a \in A$ such that*

$$a \cdot m_i = m'_i, \quad \forall i = 1, \ldots, n.$$

Let us note that the assertion of the theorem for $n = 1$ is a triviality: it says that for a non-zero vector m, the set $A \cdot m \subset M$ is all of M. But $A \cdot m$ is clearly an A-submodule, which by irreducibility is all of M.

Before we proceed to the proof of Theorem 10.2.8, let us discuss what it entails.

First, we notice that if M is an A-module such that the action map

$$A \to \mathrm{End}_k(M),$$

is surjective, then M is an irreducible A-module. (Indeed, M contains no vector subspaces invariant under all endomorphisms: given any nonzero vector, one can

send it anywhere one desires with an endomorphism upon extending this nonzero vector to a basis.)

We now claim that the converse is true:

Theorem 10.2.9 (Burnside)**.** *If M is an irreducible A-module, then the map $A \to \mathrm{End}_k(M)$ is surjective.*

Proof. Let T be a k-linear endomorphism of M. We need to find an element of A that acts on M as T. Choose a basis $m_1, \ldots, m_n$ of M as a k-vector space. Set $m_i' = T(m_i)$. By Theorem 10.2.8, there exists an element $a \in A$ such that

$$a \cdot m_i = m_i', \quad \forall i = 1, \ldots, n.$$

Then $a \cdot m_i = T(m_i)$, so a and T agree on a basis, and hence coincide. □

Week 5, Problem 9. *Give a counterexample to Theorem 10.2.9 when k is not algebraically closed.*

10.3. **Proof of Theorem 10.2.8.**

10.3.1. Set $V := k^{\oplus n}$ with basis $e_1, \ldots, e_n$. Consider the vector

$$w := m_1 \otimes e_1 + \cdots + m_n \otimes e_n \in M \otimes V.$$

Lemma 10.3.2. *The subset $A \cdot w \subset M \otimes V$ equals all of $M \otimes V$.*

Proof. The subset $A \cdot w \subset M \otimes V$ is an A-submodule. By Theorem 10.2.6 it is then of the form $M \otimes V'$ for a subspace $V' \subset V$. So we need to show that $V' = V$. Suppose not. Let $\xi : V \to k$ be a nonzero functional such that $\xi|_{V'} = 0$. Consider the map of vector spaces

$$\mathrm{id}_M \otimes \xi : M \otimes V \to M.$$

By assumption,

$$(\mathrm{id}_M \otimes \xi)|_{M \otimes V'} = 0.$$

In particular, $(\mathrm{id}_M \otimes \xi)(w) = 0$. However,

$$(\mathrm{id}_M \otimes \xi)(w) = \xi(e_1) \cdot m_1 + \ldots + \xi(e_n) \cdot m_n.$$

Since $\xi \neq 0$, at least one $\xi(e_i) \neq 0$. Hence, we obtain a nontrivial linear dependence:

$$\sum_{i=1}^{m} \xi(e_i) \cdot m_i = 0.$$

But the m_i were assumed to be linearly independent. Contradiction. □

10.3.3. Applying Lemma 10.3.2, there exists $a \in A$ such that

$$a \cdot w = w',$$

where

$$w' := m_1' \otimes e_1 + \cdots + m_n' \otimes e_n \in M \otimes V.$$

The claim is that $a \cdot m_i = m_i'$ for every i. Indeed, let $e_i^* \in V^*$ be the dual basis element. Consider the corresponding map

$$\mathrm{id}_M \otimes e_i^* : M \otimes V \to M.$$

We have

$$(\mathrm{id}_M \otimes e_i^*)(a \cdot w) = (\mathrm{id}_M \otimes e_i^*)(a \cdot m_1 \otimes e_1 + \cdots + a \cdot m_n \otimes e_n) = a \cdot m_i,$$

while

$$(\mathrm{id}_M \otimes e_i^*)(m_1' \otimes e_1 + \cdots + m_n' \otimes e_n) = m_i',$$

as required.

□

10.4. **Tensor products of algebras and irreducibility.** In this subsection the field k will still be assumed algebraically closed, and all modules will again be assumed finite-dimensional as k-vector spaces.

10.4.1. Let A_1 and A_2 be two k-algebras. We will prove the following theorem:

Theorem 10.4.2.

(a) *If M_1 and M_2 are irreducible modules over A_1 and A_2, respectively, then $M_1 \otimes M_2$ is irreducible over $A_1 \otimes A_2$.*

(b) *Let M_1, M_2 and M_1', M_2' be two pairs of irreducible modules (over A_1 and A_2, respectively). If*

$$M_1 \otimes M_2 \cong M_1' \otimes M_2'$$

as $A_1 \otimes A_2$-modules, then

$$M_1 \cong M_1' \text{ and } M_2 \cong M_2'$$

as modules over A_1 and A_2, respectively.

(c) *Any irreducible module over $A_1 \otimes A_2$ is isomorphic to one of the form $M_1 \otimes M_2$ for some M_1 and M_2 irreducible modules over A_1 and A_2, respectively.*

10.4.3. *Proof of point (a).* Let M' be a nonzero $A_1 \otimes A_2$-submodule of $M_1 \otimes M_2$. Let us consider M' and $M_1 \otimes M_2$ just as A_1-modules. From Theorem 10.2.6, we obtain that M' is of the form $M_1 \otimes M_2'$ for a nonzero vector subspace $M_2' \subset M_2$.

Similarly, considering just the action of A_2, we obtain that M' is of the form $M_1' \otimes M_2$ for a nonzero vector subspace $M_1' \subset M_1$.

By Problem 8, we obtain that

$$M_1' \otimes M_2 = M_1' \otimes M_2' = M_1 \otimes M_2'.$$

Hence $M_2 = M_2'$ and $M_1 = M_1'$.

□

10.4.4. *Proof of point (b).* Let us show that $M_1 \simeq M_1'$. Considering just the action of A_1, we have

$$M_1 \otimes M_2 \cong M_1^{\oplus n} \text{ and } M_1' \otimes M_2' \cong {M_1'}^{\oplus n'}.$$

As in the proof of 10.2.6, the existence of a nonzero map

$$M_1 \otimes M_2 \to M_1' \otimes M_2'$$

implies that $M_1 \cong M_1'$ by irreducibility.

The fact that $M_2 \cong M_2'$ is proved similarly.

□

10.4.5. *Proof of point (c).* View M first as an A_1-module. Let $M_1 \subset M$ be an irreducible A_1-submodule (e.g., take the A_1-submodule of minimal nonzero dimension as a k-vector space).

Consider the vector space $\mathrm{Hom}_{A_1}(M_1, M)$. It acquires a structure of A_2-module via the action of A_2 on M. Namely, for $T : M_1 \to M$ and $a_2 \in A_2$, we set $a_2 \cdot T$ to be the map taking $m_1 \in M_1$ to $a_2 \cdot T(m_1) \in M$. The resulting map $a_2 \cdot T$ belongs to $\mathrm{Hom}_{A_1}(M_1, M)$ since A_1 and A_2 commute in $A_1 \otimes A_2$.

In the same way, let M_2 be an irreducible A_2-submodule of $\mathrm{Hom}_{A_1}(M_1, M)$. Consider the pairing

$$M_1 \times M_2 \to M \text{ via } (m_1, T) \mapsto T(m_1).$$

This is k-bilinear, so it defines a map of vector spaces

$$M_1 \otimes M_2 \to M. \tag{10.3}$$

Note that, in fact, (10.3) is $A_1 \otimes A_2$-equivariant. By construction, it is also a *nonzero* map.

Now, by point (a), $M_1 \otimes M_2$ is irreducible as an $A_1 \otimes A_2$-module. Hence (10.3) is an isomorphism.

□

Remark 10.4.6. For the validity of Theorem 10.4.2, it is crucial that k is assumed algebraically closed. We will see how point (a) fails when we study Galois theory.

Week 5, Problem 10. *Take $A = k[t]$, and let $M = A$. Show that M does not contain non-zero irreducible submodules. Do the same for $A = \mathbb{Z}$.*

11. Tuesday, March 5

11.1. **Orthogonality of characters.**

Week 6, Problem 1. *Let G be a finite group. Show that any irreducible representation of G is finite-dimensional. (Hint: try proving the stronger fact that the dimension is bounded by $|G|$.)*

Let π be a finite-dimensional representation of a group G. Recall the function ch_π on G, defined by $\mathrm{ch}_\pi(g) := \mathrm{tr}(\pi(g))$.

Our goal is to prove the following theorem:

Theorem 11.1.1. *Let G be a finite group and let π_1 and π_2 be irreducible G-representations. Then:*

$$\sum_{g \in G} \mathrm{ch}_{\pi_1}(g) \cdot \mathrm{ch}_{\pi_2}(g^{-1}) = \begin{cases} |G| \cdot \dim(\mathrm{End}_G(\pi)) & \pi_1 \cong \pi_2 \cong \pi \\ 0 & \pi_1 \not\cong \pi_2 \end{cases} \tag{11.1}$$

as elements of k.

In the statement of the theorem the element $|G| \in k$ is understood as

$$\underbrace{1 + \cdots + 1}_{|G|} \in k, \tag{11.2}$$

and similarly for $\dim(\mathrm{End}_G(\pi)) \in k$. (That is to say, we use the canonical map $\mathbb{Z} \to k$ given by the ring structure of k.)

Corollary 11.1.2. *Assume that k is algebraically closed. Then the expression in* (11.1) *equals*

$$\begin{cases} |G| & \pi_1 \cong \pi_2 \\ 0 & \pi_1 \not\cong \pi_2. \end{cases}$$

Proof. Apply Schur's lemma. □

Week 6, Problem 2. *Show that for any finite-dimensional representation π and $g \in G$, we have*

$$\mathrm{ch}_\pi(g) = \mathrm{ch}_{\pi^*}(g^{-1}).$$

The rest of this subsection is devoted to the proof of Theorem 11.1.1.

11.1.3. Let π be a finite-dimensional representation of a group G, occurring on a vector space V. Recall the matrix coefficient map

$$\mathrm{MC}_\pi : V^* \otimes V \to \mathrm{Fun}(G, k).$$

Lemma 11.1.4. *Let π_1 and π_2 be two finite-dimensional representations. Show that the following diagram commutes*

$$\begin{array}{ccc} (V_1^* \otimes V_1) \otimes (V_2^* \otimes V_2) & \xrightarrow{\mathrm{MC}_{\pi_1} \otimes \mathrm{MC}_{\pi_2}} & \mathrm{Fun}(G,k) \otimes \mathrm{Fun}(G,k) \\ \sim\downarrow & & \downarrow \\ (V_1 \otimes V_2)^* \otimes (V_1 \otimes V_2) & \xrightarrow{\mathrm{MC}_{\pi_1 \otimes \pi_2}} & \mathrm{Fun}(G,k), \end{array}$$

where the left vertical arrow comes from the isomorphism of [Week 3, Problem 5], and the right vertical arrow is the map given by the multiplication of functions

$$f_1 \otimes f_2 \mapsto f_1 \cdot f_2.$$

Week 6, Problem 3. *Prove Lemma 11.1.4.*

Recall now that for a finite-dimensional vector space V, there is a canonical element

$$u_V \in V^* \otimes V,$$

that corresponds to $\mathrm{Id}_V \in \mathrm{End}(V)$ under the isomorphism

$$V^* \otimes V \to \mathrm{End}(V).$$

Lemma 11.1.5. *For a pair of finite-dimensional vector spaces V_1 and V_2, under the isomorphism*

$$(V_1^* \otimes V_1) \otimes (V_2^* \otimes V_2) \simeq (V_1 \otimes V_2)^* \otimes (V_1 \otimes V_2)$$

the element $u_{V_1} \otimes u_{V_2}$ corresponds to $u_{V_1 \otimes V_2}$.

Proof. We have a commutative diagram

$$\begin{array}{ccc} (V_1^* \otimes V_1) \otimes (V_2^* \otimes V_2) & \longrightarrow & \mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \\ \downarrow & & \downarrow \\ (V_1 \otimes V_2)^* \otimes (V_1 \otimes V_2) & \longrightarrow & \mathrm{End}(V_1 \otimes V_2), \end{array}$$

where the right vertical map sends $T_1 \otimes T_2$, as element of $\mathrm{End}(V_1) \otimes \mathrm{End}(V_2)$ to the linear map

$$T_1 \otimes T_2 : V_1 \otimes V_2 \to V_1 \otimes V_2$$

(sorry for the clash of notations!). Check this!

Now, the assertion of the lemma follows from the fact that

$$\mathrm{Id}_{V_1} \otimes \mathrm{Id}_{V_2} = \mathrm{Id}_{V_1 \otimes V_2}$$

as maps $V_1 \otimes V_2 \to V_1 \otimes V_2$.

□

11.1.6. Combining Lemmas 11.1.4 and 11.1.5 with Problem 2 and [Week 4, Problem 8], we reformulate the assertion of Theorem 11.1.1 as follows:

$$\sum_{g \in G} \mathrm{ch}_{\pi_1 \otimes \pi_2^*}(g) = \begin{cases} |G| \cdot \dim(\mathrm{End}_G(\pi)) & \pi_1 \cong \pi_2 \cong \pi, \\ 0 & \pi_1 \not\cong \pi_2. \end{cases} \tag{11.3}$$

We will prove the following assertion:

Theorem 11.1.7. *For a finite-dimensional representation π, we have*

$$\sum_{g \in G} \mathrm{ch}_\pi(g) = |G| \cdot \dim(\pi^G).$$

Let us show how Theorem 11.1.7 implies Theorem 11.1.1:

Proof of Theorem 11.1.1. We apply Theorem 11.1.7 to $\pi := \pi_1 \otimes \pi_2^*$. We only need to show that

$$\dim((\pi_1 \otimes \pi_2^*)^G) = \begin{cases} |G| \cdot \dim(\mathrm{End}_G(\pi)) & \pi_1 \cong \pi_2 \cong \pi, \\ 0 & \pi_1 \not\cong \pi_2. \end{cases}$$

However,

$$\pi_1 \otimes \pi_2^* \simeq \underline{\mathrm{Hom}}(\pi_2, \pi_1),$$

and hence

$$(\pi_1 \otimes \pi_2^*)^G \simeq (\underline{\mathrm{Hom}}(\pi_2, \pi_1))^G \simeq \mathrm{Hom}_G(\pi_2, \pi_1).$$

Now recall that π_1 and π_2 were irreducible, and hence a nontrivial map between them would automatically be an isomorphism.

□

11.2. **The averaging operator and the proof of Theorem 11.1.7.**

11.2.1. For a finite group G and a representation π occuring on a vector space V, we introduce an operator

$$\widetilde{\mathrm{Av}}_{G,\pi} : V \to V$$

by the formula

$$\widetilde{\mathrm{Av}}_{G,\pi}(v) = \sum_{g \in G} g \cdot v.$$

11.2.2. The following assertion is immediate from the defintion of ch_π and the linearity of the trace:

Lemma 11.2.3. *For a finite-dimensional representation π, we have*

$$\sum_{g \in G} \mathrm{ch}_\pi(g) = \mathrm{Tr}\left(\widetilde{\mathrm{Av}}_{G,\pi} \,|\, V\right).$$

11.2.4. Note that the operator $\widetilde{\mathrm{Av}}_{G,\pi}$ has the following important property:

$$\mathrm{Im}\left(\widetilde{\mathrm{Av}}_{G,\pi}\right) \subset \pi^G. \tag{11.4}$$

Note also that

$$\widetilde{\mathrm{Av}}_{G,\pi}|_{\pi^G} = |G| \cdot \mathrm{Id}_{\pi^G}. \tag{11.5}$$

11.2.5. We are now ready to prove Theorem 11.1.7.

Proof. Taking into account Lemma 11.2.3, we need to show that

$$\mathrm{Tr}\left(\widetilde{\mathrm{Av}}_{G,\pi} \,|\, V\right) = |G| \cdot \dim(\pi^G).$$

Note that if V is a finite-dimensional vector space and $T : V \to V$ is such that $\mathrm{Im}(T) \subset V'$ for a subspace $V' \subset V$, then

$$\mathrm{Tr}(T \,|\, V) = \mathrm{Tr}(T|_{V'} \,|\, V').$$

Indeed, if we denote by i the tautological embedding $V' \to V$ and by T' the map $V \to V'$ so that $T = i \circ T'$ (i.e., T thought of as landing in V'), we have

$$\mathrm{Tr}(T \,|\, V) = \mathrm{Tr}(i \circ T' \,|\, V) = \mathrm{Tr}(T' \circ i \,|\, V') = \mathrm{Tr}(T|_{V'} \,|\, V').$$

We apply this to $V' = \pi^G$ and $T = \widetilde{\mathrm{Av}}_{G,\pi}$. Now the required equality follows from (11.5).

□

11.2.6. For the rest of this section we will impose the assumption that $\mathrm{char}(k)$ does not divide $|G|$ (i.e., $|G| \neq 0$ in k). That is, we can divide by the element $|G|$ now. In this case, for a representation π occurring on a vector space V, we introduce the operator

$$\mathrm{Av}_{G,\pi} : V \to V$$

via

$$\mathrm{Av}_{G,\pi} = \frac{1}{|G|} \cdot \widetilde{\mathrm{Av}}_{G,\pi}.$$

11.2.7. Recall that if M is an abelian group, an endomorphism $S : M \to M$ is said to be an idempotent if $S^2 = S$. In this case we have

$$\ker(S) = \mathrm{Im}(\mathrm{Id} - S),$$

and

$$\ker(S) \oplus \mathrm{Im}(S) \to M \tag{11.6}$$

is an isomorphism. Namely, an element $m \in M$ is uniquely expressed as $(m - Sm) + Sm$. (If $m = k + S(n)$, then $S(m) = S(n)$ and hence $k = m - S(m)$. Hence uniqueness.)

Lemma 11.2.8. $\mathrm{Av}_{G,\pi}$ *is an idempotent, and* $\mathrm{Im}(\mathrm{Av}_{G,\pi}) = \pi^G$.

Proof. Combine (11.4) and (11.5). □

Week 6, Problem 4. *Show that the map* $\mathrm{Av}_{G,\pi} : V \to V$ *factors as*

$$V \twoheadrightarrow \pi_G \to \pi^G \hookrightarrow V,$$

and that the resulting map $\pi_G \to \pi^G$ *is an isomorphism. Show that, for a map of representations* $T : \pi_1 \to \pi_2$*, the following diagram commutes:*

$$\begin{array}{ccc} (\pi_1)_G & \longrightarrow & \pi_1^G \\ \downarrow & & \downarrow \\ (\pi_2)_G & \longrightarrow & \pi_2^G. \end{array}$$

11.3. **Complete reducibility of representations.** In this subsection the group G is finite and we continue to assume that $\mathrm{char}(k)$ does not divide $|G|$.

We will prove the following result:

Theorem 11.3.1. *(Maschke's theorem) Every finite-dimensional representation of* G *is completely reducible, i.e. is isomorphic to a direct sum of irreducible representations.*

The rest of this subsection is devoted to the proof of this theorem.

11.3.2. We will first prove the following:

Theorem 11.3.3. *Let* $T : \pi_1 \to \pi_2$ *be a surjection of finite-dimensional representations. Then the induced map*

$$\pi_1^G \to \pi_2^G$$

is also surjective.

1st proof. For any group (not necessarily finite), if $T : \pi_1 \to \pi_2$ is a surjection, then so is the induced map on quotients

$$(\pi_1)_G \to (\pi_2)_G.$$

Week 6, Problem 5. *Complete the proof using Problem 4.*

□

2nd proof. Let π_i occur on vector space V_i. Write

$$V_i = \mathrm{Im}(\mathrm{Av}_{G,\pi_i}) \oplus \ker(\mathrm{Av}_{G,\pi_i}),$$

where $\mathrm{Im}(\mathrm{Av}_{G,\pi_i}) = \pi_i^G$.

Note that

$$T \circ \mathrm{Av}_{G,\pi_1} \circ \mathrm{Av}_{G,\pi_2} \circ T.$$

Hence T maps $\mathrm{Im}(\mathrm{Av}_{G,\pi_1})$ to $\mathrm{Im}(\mathrm{Av}_{G,\pi_2})$ and $\ker(\mathrm{Av}_{G,\pi_1})$ to $\ker(\mathrm{Av}_{G,\pi_2})$.

Hence, T is surjective if and only if both maps

$$\mathrm{Im}(\mathrm{Av}_{G,\pi_1}) \to \mathrm{Im}(\mathrm{Av}_{G,\pi_2}) \text{ and } \ker(\mathrm{Av}_{G,\pi_1}) \to \ker(\mathrm{Av}_{G,\pi_2})$$

are surjective.

□

11.3.4. We are now ready to prove Theorem 11.3.1:

Proof. By [Week 5, Problem 4] and the splitting lemma, we need to show that if π is a finite-dimensional representation and $\pi' \overset{i}{\hookrightarrow} \pi$ is a sub-representation, then there exists

$$q \in \mathrm{Hom}_G(\pi, \pi')$$

such that $q \circ i = \mathrm{Id}_\pi$.

Consider the map of representations

$$\underline{\mathrm{Hom}}(\pi, \pi') \to \underline{\mathrm{Hom}}(\pi', \pi'),$$

given by precomposition with i.

We claim that it is surjective. (Note that this is all we need to show!) Indeed, the underlying map of vector spaces is

$$\mathrm{Hom}(V, V') \to \mathrm{Hom}(V', V'),$$

and this is surjective because $V' \subset V$ admits a direct sum complement on the level of vector spaces (i.e., forgetting the group action).

Hence, by Theorem 11.3.3, the map

$$\underline{\mathrm{Hom}}(\pi, \pi')^G \to \underline{\mathrm{Hom}}(\pi', \pi')^G$$

is surjective as well. That is to say,

$$\mathrm{Hom}_G(\pi, \pi') \to \mathrm{Hom}_G(\pi', \pi')$$

is a surjection.

Hence the element $\mathrm{Id}_{\pi'} \in \mathrm{Hom}_G(\pi', \pi')$ admits a preimage in $\mathrm{Hom}_G(\pi, \pi')$, as required.

□

11.3.5. The proof of Theorem 11.3.1 given above may come across as too high-tech. Here is a more down-to-earth version. We need to find a map $q : V \to V'$ which is G-invariant and such that $q \circ i = \mathrm{Id}_{V'}$. Let $T : V' \to V$ be some linear map such that $T \circ i = \mathrm{Id}_{V'}$ (this always exists on the level of vector spaces: short exact sequences of vector spaces split!). Set

$$q := \frac{1}{|G|} \sum_{g \in G} g \circ T \circ g^{-1}.$$

Then q is G-invariant by construction. Moreover,

$$\begin{aligned} q \circ i &= \frac{1}{|G|} \sum_{g \in G} g \circ T \circ g^{-1} \circ i \\ &= \frac{1}{|G|} \sum_{g \in G} g \circ T \circ i \circ g^{-1} \\ &= \frac{1}{|G|} \sum_{g \in G} g \circ \mathrm{Id}_{V'} \circ g^{-1} \\ &= \frac{1}{|G|} \sum_{g \in G} g \circ g^{-1} \\ &= \mathrm{Id}_{V'}, \end{aligned}$$

as required (note that we have used equivariance of i above).

12. Thursday, March 7

In this section G will be a finite group, k will be an algebraically closed field, and we will assume that $\mathrm{char}(k)$ does not divide $|G|$. Hence we may apply both Schur's lemma and Maschke's theorem freely.

12.1. **Decomposition of the regular representation.** Write, as usual, $\mathrm{Irrep}(G)$ for the set of isomorphism classes of nonzero irreducible representations of G. For each $\alpha \in \mathrm{Irrep}(G)$, pick a representative π_α.

12.1.1. We claim:

Proposition 12.1.2. *Let π be a finite-dimensional representation of G. Then there is a canonical isomorphism*

$$\pi \simeq \bigoplus_{\alpha \in \mathrm{Irrep}(G)} \pi_\alpha \otimes M_\alpha,$$

where $M_\alpha := \mathrm{Hom}_G(\pi_\alpha, \pi)$. Moreover, for a pair of finite-dimensional representations π' and π'' we have

$$\mathrm{Hom}_G(\pi', \pi'') \simeq \bigoplus_{\alpha \in \mathrm{Irrep}(G)} \mathrm{Hom}_k(M'_\alpha, M''_\alpha).$$

Proof. The isomorphism

$$\pi \simeq \bigoplus_{\alpha \in \mathrm{Irrep}(G)} \pi_\alpha \otimes M'_\alpha,$$

for some vector spaces M'_α follows from the complete irreducibility. We need to establish a canonical isomorphism $M'_\alpha \simeq \mathrm{Hom}_G(\pi_\alpha, \pi)$. This follows from 10.2.2.

The second assertion of the proposition follows from Proposition 10.2.2.

□

Week 6, Problem 6. *Show that, for a finite-dimensional representation π, $\dim_k(\mathrm{End}_G(\pi)) = 1$ if and only if π is irreducible. Similarly, show that*

$$\frac{1}{|G|} \sum_{g \in G} \mathrm{ch}_\pi(g)\, \mathrm{ch}_\pi(g^{-1}) = 1$$

if and only if π is irreducible.

12.1.3. We now consider $\mathrm{Reg}(G)$ — as a representation of $G \times G$. We claim:

Theorem 12.1.4. *The maps of $G \times G$ representations*

$$\mathrm{MC}_{\pi_\alpha} : \pi_\alpha \otimes (\pi_\alpha)^* \to \mathrm{Reg}(G)$$

define an isomorphism

$$\bigoplus_{\alpha \in \mathrm{Irrep}(G)} \pi_\alpha \otimes (\pi_\alpha)^* \simeq \mathrm{Reg}(G). \tag{12.1}$$

Proof. By Theorem 10.4.2, every irreducible representation of $G \times G$ is uniquely of the form $\pi_\alpha \otimes \pi_\beta$ for $\alpha, \beta \in \mathrm{Irrep}(G)$.

By Proposition 12.1.2, it is enough to show that

$$\mathrm{Hom}_{G\times G}(\pi_\alpha \otimes \pi_\beta, \mathrm{Reg}(G)) = 0$$

for $\pi_\beta \not\simeq (\pi_\alpha)^*$, and that the map MC_{π_α} spans

$$\mathrm{Hom}_{G\times G}(\pi_\alpha \otimes (\pi_\alpha)^*, \mathrm{Reg}(G)).$$

Both facts follow from Proposition 8.3.3.

□

Corollary 12.1.5. *The set* $\mathrm{Irrep}(G)$ *is finite.*

Corollary 12.1.6.

$$|G| = \sum_{\alpha \in \mathrm{Irrep}(G)} (\dim_k \pi_\alpha)^2 .$$

12.2. **The space of invariant functions.**

12.2.1. We let $\mathrm{Fun}(G,k)^G$ denote the space of functions on G that are invariant with respect to the diagonal copy of $G \subset G \times G$. That is to say, these are the functions f that satisfy

$$f(g \cdot g_1 \cdot g^{-1}) = f(g), \quad g, g_1 \in G,$$

or, equivalently,

$$f(g_1 \cdot g_2) = f(g_2 \cdot g_1).$$

Another way to say this is that f is constant on conjugacy classes. These are also called *class functions*.

12.2.2. From Theorem 12.1.4, we obtain:

Theorem 12.2.3. *The elements* $\mathrm{ch}_{\pi_\alpha} \in \mathrm{Fun}(G,k)$ *are invariant and form a basis of* $\mathrm{Fun}(G,k)^G$.

Proof. Take G-invariants on both sides of (12.1). By [Week 4, Problem 8], ch_{π_α} is the image under MC_{π_α} of the canonical element $u_{V_\alpha} \in V_\alpha^* \otimes V_\alpha$ corresponding to the identity map $V_\alpha \to V_\alpha$, where V_α is the vector space on which π_α occurs.

To prove the theorem it remains to show that u_{V_α} spans $(\pi_\alpha \otimes (\pi_\alpha)^*)^G$. As a representation of the diagonal G, we have

$$\pi_\alpha \otimes (\pi_\alpha)^* \simeq \underline{\mathrm{Hom}}(\pi_\alpha, \pi_\alpha),$$

and u_{V_α} corresponds to $\mathrm{Id}_{\pi_\alpha} \in \underline{\mathrm{Hom}}(\pi_\alpha, \pi_\alpha)$. Hence,

$$(\pi_\alpha \otimes (\pi_\alpha)^*)^G \simeq (\underline{\mathrm{Hom}}(\pi_\alpha, \pi_\alpha))^G \simeq \mathrm{Hom}_G(\pi_\alpha, \pi_\alpha).$$

Now the assertion follows from Schur's lemma: Id_{π_α} spans $\mathrm{Hom}_G(\pi_\alpha, \pi_\alpha)$.

□

Corollary 12.2.4. *The number of isomorphism classes of irreducible representations is equal to the number of conjugacy classes in G. That is to say,*

$$|\,\mathrm{Irrep}(G)| = |G/^{\mathrm{Ad}}G|,$$

where "Ad*" denotes the action of G on itself via conjugation.*

Proof. By taking dimensions, it is enough to show that $\dim_k(\mathrm{Fun}(G,k)^G)$ is the number of conjugacy classes in G. But this is obvious: just as the vector space $\mathrm{Fun}(G,k)$ has a basis given by the characteristic functions of the singleton sets, the vector space $\mathrm{Fun}(G,k)^G$ has a basis given by the characteristic functions of the conjugacy classes. Namely, to a conjugacy class $\mathbf{O}$ we associate the class function

$$f_{\mathbf{O}}(g) = \begin{cases} 1 & g \in \mathbf{O} \\ 0 & g \notin \mathbf{O} \end{cases},$$

and these are evidently a basis.

□

12.3. **Spectral projectors.** As we saw in our study of endomorphisms of vector spaces, knowing the existence of a Jordan canonical form is great and all, but we'd rather have access to the projection maps explicitly as well, if only to allow us to do calculations if necessary. The same goes for the theory we've developed: now that we have a direct sum decomposition, we'd like to make it more explicit. As for the Jordan theory, we'll call these projection maps "spectral projectors."

12.3.1. Let π be a finite-dimensional representation. Write

$$\pi \simeq \pi^{\mathrm{triv}} \oplus \pi^{\text{non-triv}},$$

where $\pi^{\mathrm{triv}} = \pi_\alpha \otimes M_\alpha$ for $\pi_\alpha \simeq \mathrm{triv}$ and $\pi^{\text{non-triv}}$ is the direct summand of all other terms.

Lemma 12.3.2. *The vector space underlying π^{triv}, viewed as a vector subspace underlying π, equals π^G.*

Proof. Obvious, since if $\pi_\alpha \neq \mathrm{triv}$, then $\pi_\alpha^G = 0$. □

Recall the operator $\mathrm{Av}_{G,\pi}$ acting on the vector space underlying π. It is easy to see that $\mathrm{Av}_{G,\pi}$ in fact belongs to $\mathrm{End}_G(\pi)$.

Lemma 12.3.3. *$\mathrm{Av}_{G,\pi}$ is the projection onto the direct summand π^{triv}. That is to say, we have*

$$\mathrm{Av}_{G,\pi}|_{\pi^{\mathrm{triv}}} = \mathrm{Id}_{\pi^{\mathrm{triv}}}$$

and

$$\mathrm{Av}_{G,\pi}|_{\pi^{\text{non-triv}}} = 0.$$

Proof. The fact that $\mathrm{Av}_{G,\pi}|_{\pi^{\mathrm{triv}}} = \mathrm{Id}_{\pi^{\mathrm{triv}}}$ is obvious.

Since $\mathrm{Av}_{G,\pi}$ is a G-endomorphism, by Proposition 12.1.2, it preserves $\pi^{\text{non-triv}}$. But since the image of $\mathrm{Av}_{G,\pi}$ belongs to π^G, the assertion follows from Lemma 12.3.2.

□

12.3.4. For $\alpha \in \mathrm{Irrep}(G)$ and a finite-dimensional representation π of G, we let π^α denote the *α-isotypic component of* π, i.e., the direct summand $\pi_\alpha \otimes M_\alpha$. We let $\pi^{\text{non-}\alpha}$ denote the direct sum of all other isotypic components. Hence

$$\pi \simeq \pi^\alpha \oplus \pi^{\text{non-}\alpha}.$$

Our current goal is to construct an element $\mathrm{pr}^\alpha \in k[G]$, such that the action of pr^α is

$$\mathrm{pr}^\alpha|_{\pi^\alpha} = \mathrm{Id}_{\pi^\alpha} \text{ and } \mathrm{pr}^\alpha|_{\pi^{\text{non-}\alpha}} = 0.$$

Note that such pr^α is automatically an element of $\mathrm{End}_G(\pi)$. We also note that for $\pi_\alpha \simeq \mathrm{triv}$, we have

$$\mathrm{pr}^\alpha = \frac{1}{|G|}\sum_{g\in G}[g],$$

so that its action on a representation π is $\mathrm{Av}_{G,\pi}$.

12.3.5. *More motivation.* Let's mention in more detail the two other famliar situations we've seen in which one has these spectral projectors.

Let V be a finite-dimensional vector space, and let $T : V \to V$ be a linear operator. For $\lambda \in k$, let $V^{(\lambda)} \subset V$ be the correponding generalized eigenspace. Recall that

$$V \simeq \bigoplus_\lambda V^{(\lambda)}.$$

Set

$$V^{\text{non-}\lambda} := \bigoplus_{\lambda'\neq\lambda} V^{(\lambda')}.$$

Then there exists a polynomial $p^\lambda(t) \in k[t]$ such that the operator $p^\lambda(T) \in \mathrm{End}(V)$ acts as follows:

$$p^\lambda(T) = \begin{cases} \mathrm{Id} \text{ on } V^{(\lambda)}, \\ 0 \text{ on } V^{\text{non-}(\lambda)}. \end{cases}$$

Moreover we wrote this polynomial down totally explicitly.

Let now A be a finite abelian group. View it as a $\mathbb{Z}$-module. Write

$$A \simeq \bigoplus_p A^{(p)},$$

where each $A^{(p)}$ is a p-group. Set

$$A^{\text{non-}p} := \bigoplus_{p'\neq p} A^{(p')}.$$

Then there exists another explicit element $N^p \in \mathbb{Z}$ that acts on A as the projection onto the $A^{(p)}$ direct summand.

We are after the same thing — but in the context of group representations.

12.3.6. Now consider the element

$$\widetilde{\mathrm{pr}}^\alpha = \frac{1}{|G|}\sum_{g\in G} \mathrm{ch}_{(\pi_\alpha)^*}(g)[g] \in k[G].$$

Theorem 12.3.7. *The element $\widetilde{\mathrm{pr}}^\alpha$ acts by 0 on any π_β with $\beta \neq \alpha$. It acts on π_α by multiplication by $\frac{1}{\dim(\pi^\alpha)}$. (In particular, $\dim(\pi^\alpha) \neq 0$ in k.)*

Proof of Theorem 12.3.7.

Step 1:

Week 6, Problem 7. *Let π_1 and π_2 be two representations such that $(\pi_1 \otimes \pi_2)^G = 0$. Adapt the proof of Theorem 11.1.1 to show that, for any $w_1 \in V_1^* \otimes V_1$ and $w_2 \in V_2^* \otimes V_2$,*

$$\sum_{g\in G} \left(\mathrm{MC}_{\pi_1}(w_1)\right)(g) \cdot \left(\mathrm{MC}_{\pi_2}(w_2)\right)(g) = 0.$$

Week 6, Problem 8. *Deduce that* $\widetilde{\mathrm{pr}}^{\alpha}$ *acts by* 0 *on any irreducible representation which is not isomorphic to* π_α.

Step 2: Let f be any element of $\mathrm{Fun}(G,k)^G$, and consider the element

$$r_f := \sum_{g\in G} f(g)[g] \in k[G].$$

The first claim is that it belongs to the *center* of G. That is to say,

$$x \cdot r_f = r_f \cdot x, \quad \forall x \in k[G].$$

It suffices to show that

$$[g_1] \cdot r_f = r_f \cdot [g_1], \quad \forall g_1 \in G.$$

But

$$\begin{aligned}
[g_1] \cdot r_f &= \sum_{g\in G} f(g) \cdot [g_1] \cdot [g] \\
&= \sum_{g\in G} f(g_1^{-1} \cdot g) \cdot [g] \\
&= \sum_{g\in G} f(g \cdot g_1^{-1}) \cdot [g] \\
&= \sum_{g\in G} f(g) \cdot [g] \cdot [g_1] \\
&= r_f \cdot [g_1].
\end{aligned}$$

Step 3: Let R be any ring and $r \in R$ an element in its center. Then for an R-module M, the action of r on M belongs to $\mathrm{End}_R(M)$ (do you see why?).

Step 4: Hence the action of $\widetilde{\mathrm{pr}}^{\alpha}$ on any π belongs to $\mathrm{End}_G(\pi)$. By Schur's lemma, when π is irreducible, the action of $\widetilde{\mathrm{pr}}^{\alpha}$ is given by multiplication by a scalar. In particular, $\widetilde{\mathrm{pr}}^{\alpha}$ acts by a scalar on π_α. We need to show that when we multiply this scalar by $\dim(\pi_\alpha)$ we obtain 1. Equivalently, we have to show that

$$\mathrm{Tr}(\widetilde{\mathrm{pr}}^{\alpha} \,|\, \pi_\alpha) = 1.$$

But

$$\mathrm{Tr}(\widetilde{\mathrm{pr}}^{\alpha} \,|\, \pi_\alpha) = \frac{1}{|G|} \sum_{g\in G} \mathrm{ch}_{(\pi_\alpha)^*}(g)\, \mathrm{ch}_{\pi_\alpha}(g) = 1,$$

by Theorem 11.1.1.

□

Just to restate the observation at the end of the theorem,

Corollary 12.3.8. *The element* $\dim(\pi_\alpha) \in k$ *is nonzero — i.e.,* $\mathrm{char}(k)$ *does not divide* $\dim(\pi_\alpha)$.

Remark 12.3.9. Here is, btw, another proof that $\widetilde{\mathrm{pr}}^{\alpha}$ acts by zero on π_β with $\beta \neq \alpha$. By Step 3, $\widetilde{\mathrm{pr}}^{\alpha}$ acts by a scalar. Since $\dim(\pi_\beta) \in k$ (which was proved

independently), it is enough to show that $\mathrm{Tr}(\widetilde{\mathrm{pr}}^{\alpha}, \pi_\beta) = 0$. However, the above trace equals

$$\frac{1}{|G|} \sum_{g \in G} \mathrm{ch}_{(\pi_\alpha)^*}(g)\, \mathrm{ch}_{\pi_\beta}(g) = 1,$$

which vanishes by Theorem 11.1.1.

12.3.10. So, with this in hand, we define

$$\mathrm{pr}^{\alpha} = \dim(\pi_\alpha) \cdot \widetilde{\mathrm{pr}}^{\alpha}.$$

This is then the sought-for spectral projector.

Week 6, Problem 9. *Show that* pr^{α} *is an idempotent in* $k[G]$*, i.e., that*

$$\mathrm{pr}^{\alpha} \cdot \mathrm{pr}^{\alpha} = \mathrm{pr}^{\alpha}.$$

12.4. **Action of the group algebra on representations.**

12.4.1. For every $\alpha \in \mathrm{Irrep}(G)$, consider the action map

$$k[G] \to \mathrm{End}_k(V_\alpha),$$

where V_α is the vector space underlying the representation π_α.

By taking the direct sum over $\alpha \in \mathrm{Irrep}(G)$, we obtain a map

$$k[G] \to \bigoplus_{\alpha \in \mathrm{Irrep}(G)} \mathrm{End}_k(V_\alpha). \tag{12.2}$$

We claim:

Theorem 12.4.2. *The map* (12.2) *is an isomorphism.*

That is to say, the group algebra is a direct sum of so-called "matrix algebras." The properties of these matrix algebras have been studied very carefully and much can be said about them — and hence much can be said about group algebras of finite groups (over an algebraically closed field of characteristic coprime to the order of a given group).

Proof. Let G be *any* group (i.e., not necessarily finite), and let π be a finite-dimensional representation. Note that we have a canonical isomorphism of vector spaces

$$(k[G])^* \simeq \mathrm{Fun}(G, k) \tag{12.3}$$

that sends a functional $\xi : k[G] \to k$ to the function f whose value on $g \in G$ is $\xi([g])$.

Note that for a finite-dimensional vector space V we have a canonical isomorphism

$$\mathrm{End}_k(V) \simeq \mathrm{End}_k(V)^*, \tag{12.4}$$

see (5.2).

Week 6, Problem 10. *Show that for a representation* π *occurring on a vector space* V*, the dual map*

$$(\mathrm{End}_k(V))^* \to (k[G])^*$$

of the action map

$$k[G] \to \mathrm{End}_k(V)$$

identifies — under (12.3) *and* (12.4) *— with the map*

$$\mathrm{End}_k(V) \simeq V \otimes V^* \xrightarrow{\mathrm{MC}_\pi} \mathrm{Fun}(G,k).$$

Hence the assertion of Theorem 12.4.2 follows from that of Theorem 12.1.4 by duality (since, for us, G is finite).

□

12.4.3. *Comparing the two isomorphisms.* The final question that we want to address is the following. Consider the isomorphism

$$\mathrm{Fun}(G,k) \simeq k[G], \quad f \mapsto \sum_{g \in G} f(g) \cdot [g]. \tag{12.5}$$

Combining Theorems 12.1.4 and 12.4.2, we obtain a sequence of isomorphisms of $G \times G$ representations.

$$\begin{aligned} \bigoplus_{\alpha \in \mathrm{Irrep}(G)} \pi_\alpha \otimes (\pi_\alpha)^* \to \mathrm{Fun}(G,k) \simeq k[G] &\to \bigoplus_{\alpha \in \mathrm{Irrep}(G)} \underline{\underline{\mathrm{Hom}}}(\pi_\alpha, \pi_\alpha) \\ &\simeq \bigoplus_{\alpha \in \mathrm{Irrep}(G)} (\pi_\alpha)^* \otimes \pi_\alpha \\ &\simeq \bigoplus_{\alpha \in \mathrm{Irrep}(G)} \pi_\alpha \otimes (\pi_\alpha)^*. \end{aligned}$$

Since all the representations involved are irreducible and pairwise nonisomorphic, the above composition maps each $\pi_\alpha \otimes (\pi_\alpha)^*$ on the left-hand side to the corresponding direct summand on the right-hand side. By Schur's lemma, this map is given by multiplication by a scalar. Call this scalar c_α.

Theorem 12.4.4.

$$c_\alpha = \frac{|G|}{\dim(\pi_\alpha)}.$$

Proof. It suffices to show that the map in question sends

$$u_{V_\alpha} \in V_\alpha^* \otimes V_\alpha$$

to

$$\frac{|G|}{\dim(\pi_\alpha)} u_{V_\alpha} \in V_\alpha^* \otimes V_\alpha.$$

So we need to calculate the action of

$$\mathrm{MC}_{\pi_\alpha}(u_{V_\alpha}) = \mathrm{ch}_{\pi_\alpha} \in \mathrm{Fun}(G,k) \simeq k[G]$$

on the representation $(\pi_\alpha)^*$. But the operator in question is

$$\frac{|G|}{\dim(\pi_\alpha)} \mathrm{pr}^\beta$$

(do you see why?), where $\pi_\beta \simeq (\pi_\alpha)^*$. Hence the assertion follows.

□

Remark 12.4.5. In fact, and this is kind of cool, if we are over an algebraically closed field of characteristic *zero*, each of these c_α's is an integer. Actually, more is true: the dimensions of the irreducible representations of G actually all divide the positive integer $\frac{|G|}{|Z(G)|}!!$ (Here $Z(G)$ is the center of G.)

13. Tuesday, March 12

Let's change focus now to studying the fields that we had to worry about above in their own right. One motivation for this is number-theoretic: given a Diophantine equation, like $x^2 - dy^2 = 1$, it was observed that in very special but tremendously beautiful cases one can transfer questions about solutions to questions about field theory. For instance, we might factor the left-hand side of our example to get $(x+y\sqrt{d})(x-y\sqrt{d}) = 1$, and then we are asking about elements of the field $\mathbb{Q}(\sqrt{d})$, which we might define provisionally as $\mathbb{Q}(\sqrt{d}) := \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}$.

Or perhaps we'd like to solve the Fermat equation $x^n + y^n = z^n$. Then we'd factor the left-hand side to get $\prod_{i=0}^{n-1}(x + y\zeta_n^i) = z^n$ and transfer to a problem in $\mathbb{Q}(\zeta_n) \supset \mathbb{Q}$, and the number theorists of the 1800s (e.g. the story of Lamé and Kummer) knew precisely the advantages (and their limits) gained from this perspective. But first let's worry about the more general picture.

13.1. **Algebraic and finite extensions of fields.**

13.1.1. Let K be a field and let $p(t) \in K[t]$ be an irreducible polynomial. We'd like to find a field in which p has a root (of course we could ask this for any polynomial, but the question immediately reduces to one about its irreducible factors). There will of course be many such fields, but there is a 'universal' one: we construct a field extension $L \supset K$ by setting

$$L_p := K[t]/p(t)K[t] = K[t]/(p),$$

where we have written $(p) := p(t)K[t]$ for the ideal generated by p. (Field extensions are often notated L/K, read L *over* K, rather than $L \supset K$, as well.)

We claim that the K-algebra L_p is indeed a field:

Proof. A commutative ring R is a field if and only if the only proper ideal in R is the zero ideal (indeed, if $0 \neq r \in R$, consider the ideal $(r) := r \cdot R \subset R$. We have $I \neq (0)$, hence $I = R$, hence $1 \in I$, and hence there exists $r' \in R$ such that $r \cdot r' = 1$).

Now, ideals in $K[t]/p(t)K[t]$ are in bijection with ideals of $K[t]$ that contain $p(t)K[t]$. However, since $p(t)$ is irreducible, the ideal $p(t)K[t]$ is maximal, and the assertion follows. (We have used here that $K[t]$ is a principal ideal domain.) □

13.1.2. The field extension $L_p \supset K$ has the following universal property. Let x_{univ} be the element of L_p equal to the image of the element $t \in K[t]$ under the projection $K[t] \to K[t]/p(t)K[t]$. Notice that $p(x_{univ}) = 0$. The claim is that L_p is the universal extension of K with a root of p.

Lemma 13.1.3. *For a field extension $L \supset K$, evaluation on x_{univ} defines a bijection between the set of ring homomorphisms $L_p \to L$ and elements $x \in L$ satisfying $p(x) = 0$.*

Proof. Do it yourself. □

13.1.4. *Algebraic elements.* Let $L \supset K$ be a field extension, and let $x \in L$ be an element. We shall say that x is algebraic over K if there exists a polynomial $p(t) \in K[t]$ such that $p(x) = 0$ (another way to say this is that its powers x^i are linearly dependent over K).

Remark 13.1.5. Note that with no restriction of generality, we can assume that the polynomial $p(t)$ above, if it exists, is irreducible. Indeed, if it is not, factor it as $\prod_i p_i(t)$, where the $p_i(t)$'s are irreducible. Since $p(x) = 0$, we obtain that $p_i(x) = 0$ for at least one index i.

Even better, such an irreducible $p(t)$ is unique up to scaling by K: it is a generator of the ideal $\{q \in K[t] : q(x) = 0 \in L\}$ of $K[t]$, which is a PID whose units are precisely the polynomials of degree 0 — i.e., the scalars. In particular, if we ask that p be monic and irreducible, then there is a unique such p, called the *minimal polynomial* of x over K.

Definition 13.1.6. *An extension $L \supset K$ is said to be algebraic if all of its elements are algebraic over K.*

Here is a typical example of a non-algebraic extension: $K(t) \supset K$, where $K(t)$ is the field of rational functions in the variable t. (That is, take $K[t]$ and take its fraction field: the field of quotients of two polynomials (called *rational functions*).) Then the element t itself is non-algebraic.

13.1.7. *Finite field extensions.* A field extension $L \supset K$ is said to be finite if L is finite-dimensional as a K-vector space. We shall call the integer $\dim_K(L)$ the *degree* of L over K, and denote it by $\deg(L/K)$ or $[L : K]$.

Evidently, $\deg(L/K) = 1$ if and only if the extension is trivial, i.e., $L = K$.

Lemma 13.1.8. *For an irreducible polynomial $p(t)$, the field extension $L_p \supset K$ is finite, of degree $[L_p : K] = \deg(p)$ (hence the name).*

Proof. We had might as well take p to be monic. (Do you see why?)

It suffices to show the elements $1, t, \ldots, t^{n-1}$, where $n = \deg(p)$, when projected to L_p, form a basis of L_p over K. Let x be the image of t in L_p.

Linear independence is easy: to have $\sum_{i=0}^{n-1} a_i x^i = 0 \in L_p$ would correspond to $\sum_{i=0}^{n-1} a_i t^i = p(t)q(t) \in K[t]$ — but if $q \neq 0$ the right-hand side has degree $\geq n$.

To see these span, certainly the powers of x span since the powers of t span $K[t]$ even before projection. But $p(x) = x^n + c_{n-1}x^{n-1} + \cdots = 0$ tells us that x^n is in the span of $1, \ldots, x^{n-1}$. Proceeding by induction, since multiplying this relation by x^k tells us that x^{n+k} is in the span of $1, \ldots, x^{n+k-1}$, we have the claim that $1, \ldots, x^{n-1}$ spans. □

Lemma 13.1.9. *Let $M \supset L \supset K$ be field extensions such that M is finite over L and L is finite over K. Then M is finite over K. Moreover,*

$$[M : K] = [M : L][L : K].$$

Iterated field extensions $M \supset L \supset K$ are often called *towers*.

Proof. More generally, if V is a finite-dimensional L-vector space and $L \supset K$ is a finite field extension, then V is finite-dimensional as a K-vector space, and

$$\dim_K(V) = \dim_L(V) \cdot \deg(L/K).$$

(Check this! Hint: choose bases.) □

Lemma 13.1.10. *Any finite extension is algebraic.*

Proof. Let $L \supset K$ be a finite field extension, and let $x \in L$. Let $n := \deg(L/K)$. Then the elements $1, x, \ldots, x^n$ are linearly dependent over K, since there are $n+1$ of them. But this precisely says that there exist elements $a_0, a_1, \ldots, a_n \in K$ such that

$$a_0 + a_1 x + \cdots + a_n x^n = 0.$$

Hence if we set

$$p(t) := a_0 + a_1 t + \cdots + a_n t^n \in K[t],$$

then $p(x) = 0$, as required.

□

Corollary 13.1.11. *For an irreducible polynomial $p(t) \in K[t]$, every element of L_p is algebraic over K.*

13.1.12. *Generation.* Let $L \supset K$ be a field extension, and let $x_1, \ldots, x_n \in L$ be elements. We shall say that these elements *generate L as a field extension* if L does not contain a proper subfield that contains both K and these elements.

In other words, every element of L can be obtained by a finite procedure of taking sums, products and inverses, starting from elements of K and $x_1, \ldots, x_n$.

In yet other words, writing $K(x_1, \ldots, x_n) \subseteq L$ for the smallest field containing K and the x_i, to say that the x_i generate L over K is precisely to say that $K(x_1, \ldots, x_n) = L$. (Check that it makes sense to say "smallest"! — i.e., check that the intersection $\cap_{L' \ni x_i} L'$ of subextensions $L \supseteq L' \supseteq K$ containing the x_i is again a field.)

Week 7, Problem 1.

(a) *Suppose that L is generated as a field extension over K by an element x that is algebraic over K. Let $p(t) \in K[t]$ be the minimal polynomial of x over K. Show that the map of fields $L_p \to L$ via $x_{univ} \mapsto x$ is an isomorphism. Deduce, in particular, that the map of K-algebras $K[t] \to L$ via $t \mapsto x$ is surjective.*

(b) *Let $L \supset K$ be a field extension, and let $x_1, \ldots, x_n \in L$. Set $L_i = K(x_1, \ldots, x_i)$. Show that L_i is generated over L_{i-1} by the element x_i.*

(c) *Let $L \supset K$ be a field extension generated by elements $x_1, \ldots, x_n \in L$ algebraic over K. Consider the map of K-algebras $K[t_1, \ldots, t_n] \to L$ via $t_i \mapsto x_i$. Show that it is surjective.*

Week 7, Problem 2. *Let K be a field, and let A be a finite-dimensional commutative K-algebra with no zero-divisors, i.e., $a_1, a_2 \neq 0$ implies $a_1 a_2 \neq 0$. Show that A is a field.*

Hint: think about the proof of Lemma 13.1.10.

Week 7, Problem 3. *Use problem 2 to give an alternative proof for Problem 1(c).*

13.1.13. *Finiteness vs. algebraicity.* We have the following key observation:

Proposition 13.1.14. *Let $L \supset K$ be a field extension. Then the following are equivalent:*

(a) *L is finite over K.*

(b) *L is algebraic and is generated by finitely many elements.*

(c) *L is generated over K by finitely many algebraic elements.*

Proof. Point (a) implies point (b) by Lemma 13.1.10 and the observation that if x_i span L as a K vector space, then they certainly generate L over K as a field as well. Point (b) implies point (c) tautologically. Let us prove that (c) implies (a).

Let $x_1, \ldots, x_n \in L$ be elements that are algebraic over K and also generate L. Define the fields

$$K = L_0 \subset L_1 \subset \ldots \subset L_{n-1} \subset L_n$$

by letting L_i be generated over K by the elements $x_1, \ldots, x_i$. By assumption, $L_n = L$.

By Lemma 13.1.9, it suffices to show that each extension $L_{i-1} \subset L_i$ is finite. Note that L_i is generated over L_{i-1} by one element (namely, x_i). Since x_i is algebraic over K, it is algebraic over L_{i-1} (use the same polynomial). By Remark 13.1.5, we can assume that x_i satisfies an irreducible polynomial $p_i(t) \in L_{i-1}[t]$. Hence, by Lemma 13.1.3, we obtain a map of field extensions of L_{i-1}:

$$(L_{i-1})_{p_i} \to L_i.$$

This map is surjective, since x_i generates L_i over L_{i-1}. Hence, $L_i \simeq (L_{i-1})_{p_i}$. (Remember that a map of fields thought of as rings is automatically injective — for instance, the kernel would be a proper ideal, hence zero.) Hence, we are done by Lemma 13.1.8.

□

Corollary 13.1.15. *Let $L \supset K$ be a field extension. Then L/K is algebraic if and only if it is a union of finite extensions of K: i.e., there exist subfields $L \supset L_i \supset K$ such that each L_i/K is finite and*

$$L = \bigcup_i L_i.$$

13.1.16. *Algebraic extensions.* We are going to prove:

Theorem 13.1.17. *Let $L \supset K$ be a field extension, and let $L' \subset L$ be the subset of elements algebraic over K. Then L' is a subfield.*

Proof. We need to show that this $L' \subset L$ is stable under addition, multiplication, and contains inverses (of course it contains $1 \in K$).

The situation with inverses is evident. If $x \neq 0$ satisfies the polynomial

$$p(t) = a_0 + a_1 t + \cdots + a_n t^n \in K[t],$$

then (multiplying $\sum a_i x^i = 0$ through by x^{-n}) we see that x^{-1} satisfies the polynomial

$$a_n + a_{n-1} t + \cdots + a_1 t^{n-1} + a_0 t^n.$$

Let now x_1 and x_2 be two elements of L that are algebraic over K. Let $K(x_1, x_2) \subset L$ be the subfield generated by them over K. By Proposition 13.1.14, $K(x_1, x_2)$ is a finite extension of K. Hence, every element of $K(x_1, x_2)$ is algebraic over K by Lemma 13.1.10. In particular, $x_1 + x_2, x_1 x_2 \in K(x_1, x_2)$ are both algebraic over K. This completes the proof.

□

We now claim:

Theorem 13.1.18. *Let $M \supset L \supset K$ be field extensions, such that M is algebraic over L and L is algebraic over K. Then M is algebraic over K.*

Proof. Let x be an element of M. Let $p(t) \in L[t]$ be a polynomial such that $p(x) = 0$. Let

$$a_0, \ldots, a_n \in L$$

be the coefficients of p. Let

$$L' := K(a_0, \ldots, a_n) \subset L$$

be the subextension of L generated over K by $a_0, \ldots, a_n$. Let

$$M' := K(a_0, \ldots, a_n, x)$$

be the subextension of M generated over K by $a_0, \ldots, a_n, x$. Then L' is finite over K by Proposition 13.1.14, and M' is finite over L' because of our hypothesis on p. Hence M' is finite over K by Lemma 13.1.9. The theorem then follows by Corollary 13.1.15. □

13.2. **Maps between extensions.** Now that we know something about how these extensions (or, at least, some interesting classes of extensions) behave under towers, let's turn to wondering about when we can put one extension inside another to try to play this tower game. For instance, $\mathbb{Q}(i) \supset \mathbb{Q}$ does not embed into $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$ (do you see why?), but $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ does.

13.2.1. Let K be a field, and let L and L' be a pair of its extensions. In this subsection we will study the set

$$\mathrm{Hom}_{K\text{-Alg}}(L, L')$$

of maps of K-algebras $L \to L'$ (remember that these are automatically injective, so we could have called these embeddings if we'd wanted). That is to say, the set of maps $L \to L'$ that take the inclusion map $K \to L$ to the inclusion map $K \to L'$.

We will prove:

Theorem 13.2.2. *Assume that L is finite over K. Then the set* $\mathrm{Hom}_{K\text{-Alg}}(L, L')$ *is finite, and has cardinality bounded by*

$$|\mathrm{Hom}_{K\text{-Alg}}(L, L')| \leq \deg(L/K).$$

Week 7, Problem 4. *Show that for $L := K(t)$ and $L' \supset K$ any extension of K, the set* $\mathrm{Hom}_{K\text{-Alg}}(L, L')$ *is in bijection with the set of* non-algebraic *(or* transcendental*) elements $x \in L'$.*

13.2.3. *Elementary proof of Theorem 13.2.2.*

Special Case. Suppose that $L = L_p \supset K$ for some irreducible polynomial p. Then the assertion follows from Lemma 13.1.3 since the polynomial p cannot have more than $\deg(p) = \deg(L/K)$ distinct roots in L' (and a map is exactly determined by a root of p in L').

General Case. We will argue by induction on $\deg(L/K)$. If $\deg(L/K) = 1$, then $L = K$ and there is nothing to prove. For $L \neq K$ pick an element $x \in L - K$. Let $L_1 := K(x) \subset L$ be the subextension generated by x. We have a map of sets

$$\mathrm{Hom}_{K\text{-Alg}}(L, L') \to \mathrm{Hom}_{K\text{-Alg}}(L_1, L'),$$

given by restriction.

Note that L_1 is as in the Special Case. Hence, $\mathrm{Hom}_{K\text{-Alg}}(L_1, L')$ is finite of cardinality at most $\deg(L_1/K)$. Since

$$\deg(L/K) = \deg(L/L_1) \cdot \deg(L_1/K),$$

it remains to show that each element

$$(\phi_1 : L_1 \to L') \in \mathrm{Hom}_{K\text{-Alg}}(L_1, L')$$

has no more than $\deg(L/L_1)$ pre-images in $\mathrm{Hom}_{K\text{-Alg}}(L, L')$ — i.e., there are at most $\deg(L/L_1)$ extensions of the embedding $L_1 \to L'$ to all of L.

Note that the element ϕ_1 makes L' into a L_1-algebra, and the set of extensions of ϕ_1 (the preimage of $\{\phi_1\}$ in $\mathrm{Hom}_{K\text{-Alg}}(L, L')$) identifies with the set

$$\mathrm{Hom}_{L_1\text{-Alg}}(L, L').$$

But then the inequality

$$|\mathrm{Hom}_{L_1\text{-Alg}}(L, L')| \leq \deg(L/L_1)$$

follows by induction.

□

13.2.4. We shall now discuss a fancier proof of Theorem 13.2.2. For this we will use a theorem from linear algebra (to be proved next time).

Before stating the theorem, let us first review the following construction. Let $R_1, \ldots, R_n$ be a finite collection of rings. We can form the ring

$$R := R_1 \oplus \cdots \oplus R_n,$$

where the addition and multiplication are defined componentwise. Hence the multiplicative unit of this ring is

$$(1_1, 1_2, \ldots, 1_n),$$

where each 1_i is the unit of R_i. Note that two elements of shape

$$(0, \ldots, r_i, \ldots, 0, 0) \text{ and } (0, 0, \ldots, r_j, \ldots, 0)$$

automatically multiply to 0 unless $i = j$.

Assume that each R_i is a K-algebra. Then so is R, where the homomorphism $K \to R$ is given by the direct sum of the homomorphisms to the R_i.

Now to the theorem.

Theorem 13.2.5. *[Structure theorem for finite dimensional K algebras.] Let A be a commutative K-algebra which is finite-dimensional as a K-vector space. Then A can be written as a direct sum of K-algebras (in the above sense)*

$$A \simeq \bigoplus_{i \in I} A_i,$$

where each A_i has the following property: A_i contains an ideal $m_i \subset A_i$, such that

- *Every element of m_i consists of nilpotent elements.*
- *The quotient A_i/m_i is a field (i.e., $m_i \subset A_i$ is a maximal ideal).*

13.2.6. Let us show how Theorem 13.2.5 implies Theorem 13.2.2.

Step 1. Consider the L'-algebra $A := L' \underset{K}{\otimes} L$, where L' maps to A by means of $x \mapsto x \otimes 1_L$.

Lemma 13.2.7. *Let $L_1 \to L_2$ be a homomorphism of fields, and let A_i be an L_i-algebra for each $i = 1, 2$. The natural map (arising from the universal property)*

$$\mathrm{Hom}_{L_1\text{-Alg}}(A_1, A_2) \to \mathrm{Hom}_{L_2\text{-Alg}}(L_2 \underset{L_1}{\otimes} A_1, A_2)$$

is an isomorphism — its inverse is given by restriction along $A_1 \hookrightarrow L_2 \underset{L_1}{\otimes} A_1$.

Proof. Same as the proof of Proposition 4.1.5. □

Thus, we need to study the set

$$\mathrm{Hom}_{L'\text{-Alg}}(A, L'),$$

with $A = L' \underset{K}{\otimes} L$ as above.

Step 2. By Theorem 13.2.5 we can write A as

$$A \simeq \bigoplus_{i \in I} A_i.$$

First, we note that

$$|I| \leq \dim_{L'}(A) = \dim_{L'}(L' \underset{K}{\otimes} L) = \dim_K(L) = \deg(L/K).$$

Now let $\widetilde{L}$ be any field. We claim that every homomorphism $\phi : A \to \widetilde{L}$ has the property that it factors as

$$A \twoheadrightarrow A_i \xrightarrow{\phi|_{A_i}} \widetilde{L}$$

for a unique $i \in I$. That is, it factors through the projection to a unique A_i. For this, it suffices to show that if $\phi|_{A_i} \neq 0$ for some i, then $\phi|_{A_j} = 0$ for every $j \neq i$. (Here, as usual, we are identifying A_k with $(0, \ldots, A_k, \ldots, 0)$.)

To see this, choose $a_i \in A_i$ so that $\phi(a_i) \neq 0$. Note that, as we noted above, for every $a_j \in A_j$ $(j \neq i)$,

$$(0, \ldots, a_i, \ldots, 0, 0) \cdot (0, 0, \ldots, a_j, \ldots, 0) = 0.$$

Hence

$$0 = \phi(0) = \phi(a_i \cdot a_j) = \phi(a_i) \cdot \phi(a_j),$$

which forces $\phi(a_j) = 0$, since $\widetilde{L}$ is a field.

Thus we obtain that

$$\mathrm{Hom}_{L'\text{-Alg}}(A, L') \simeq \coprod_{i \in I} \mathrm{Hom}_{L'\text{-Alg}}(A_i, L'),$$

the disjoint union of these sets.

Step 3. So we have reduced to the claim that, for every i, the set $\mathrm{Hom}_{L'\text{-Alg}}(A_i, L')$ contains no more than one element.

Since $m_i \subset A_i$ consists of nilpotent elements, every homomorphism $\phi : A_i \to L'$ annihilates m_i. Hence ϕ factors through a map of fields $\overline{\phi} : A_i/m_i \to L'$, whose precomposition with

$$\psi : L' \hookrightarrow A_i \twoheadrightarrow A_i/m_i$$

is the identity map on L'. Since $\overline{\phi}$ is injective (it is a map of fields), we obtain that ψ is an isomorphism, and $\overline{\phi}$ is its (unique) inverse. Hence, *if* such a map ϕ exists (and it may not!), it is automatically the unique inverse to the isomorphism $\psi : L' \to A_i/m_i$.

□

13.2.8. From the second proof of Theorem 13.2.2 we obtain the following explicit description of the set

$$\mathrm{Hom}_{K\text{-Alg}}(L, L') \simeq \mathrm{Hom}_{L'\text{-Alg}}(L' \underset{K}{\otimes} L, L').$$

Namely, consider the subset $I' \subset I$ that consists of those i for which the map

$$L' \to L' \underset{K}{\otimes} L =: A \to A_i \to A_i/m_i$$

is an isomorphism.

Note that each $i \in I'$ defines a homomorphism of L'-algebras.

$$A \to A_i \to A_i/m_i \simeq L'.$$

Week 7, Problem 5. *Show that the above map $I' \to \mathrm{Hom}_{L'\text{-Alg}}(L' \underset{L}{\otimes} L, L')$ is a bijection.*

Corollary 13.2.9. *The equality $|\mathrm{Hom}_{K\text{-Alg}}(L, L')| = \deg(L/K)$ holds* if and only if *each A_i is isomorphic to L' (in particular, all $m_i = 0$).*

Proof. Note that

$$\begin{aligned}
\deg(L/K) &= \dim_{L'}(A) \\
&= \sum_i \dim_{L'}(A_i) \\
&\geq \sum_i \dim_{L'}(A_i/m_i) \\
&\geq |I'| \\
&= |\mathrm{Hom}_{K\text{-Alg}}(L, L')|,
\end{aligned}$$

where the first inequality is an equality if and only if all $m_i = 0$, and the second inequality is an equality if and only if all $\dim_{L'}(A_i/m_i) = 1$.

□

13.2.10. With these out of the way, let us now prove the theorem.

13.3. **Proof of Theorem 13.2.5.**

13.3.1. First, we recall the following statement from linear algebra. Let V be a finite-dimensional K-vector space and let $T : V \to V$ be an endomorphism. Then we can (canonically) split V as a direct sum of T-invariant vector subspaces

$$V^{T\text{-nilp}} \oplus V^{T\text{-inv}},$$

where T acts nilpotently on $V^{T\text{-nilp}}$ and invertibly on $V^{T\text{-inv}}$. In fact

$$V^{T\text{-nilp}} = \ker(T^N) \text{ and } V^{T\text{-inv}} = \mathrm{Im}(T^N)$$

for any $N \geq \dim(V)$. See Notes for Math 122, Theorem 8.6.8 for the proof.

13.3.2. Let $S : V \to V$ be an operator that commutes with T. Then the vector spaces $V^{T\text{-nilp}}$ and $V^{T\text{-inv}}$ are S-invariant. Hence, we can apply to each of them a similar decomposition with respect to the action of S.

We obtain a direct sum decomposition of V into subspaces that are both S and T-invariant

$$V \simeq V^{T\text{-nilp},S\text{-nilp}} \oplus V^{T\text{-inv},S\text{-nilp}} \oplus V^{T\text{-nilp},S\text{-inv}} \oplus V^{T\text{-inv},S\text{-inv}}.$$

13.3.3. By induction, for any finite family $T_i,\ i \in I$ of pairwise commuting operators, we obtain a direct sum decomposition V into subspaces that are invariant with respect to all of these operators:

$$V = \bigoplus_{I=I_1 \sqcup I_2} V^{I_1\text{-nilp},I_2\text{-inv}},$$

where on the direct summand $V^{I_1\text{-nilp},I_2\text{-inv}}$ the operators $T_i,\ i \in I_1$ act nilpotently, and the operators $T_i,\ i \in I_2$ act invertibly.

13.3.4. Let now $T_i,\ i \in I$ be a possibly infinite collection of pairwise commuating operators. We claim that, thanks to the finite-dimensionality of V, we still have a direct sum decomposition V into subspaces that are invariant with respect to all of these operators:

$$V = \bigoplus_{I=I_1 \sqcup I_2} V^{I_1\text{-nilp},I_2\text{-inv}}.$$

Indeed, consider such decompositions for all finite subsets $I' \subset I$, and take one

$$V = \bigoplus_{I'=I'_1 \sqcup I'_2} V^{I'_1\text{-nilp},I'_2\text{-inv}} \tag{13.1}$$

that has maximally many nonzero terms (a maximum exists by finite dimensionality). We claim that this decomposition has the required property.

Namely, we claim that for each direct summand, $V^{I'_1\text{-nilp},I'_2\text{-inv}}$ and any element $i \in I$, the operator T_i acts on $V^{I'_1\text{-nilp},I'_2\text{-inv}}$ either nilpotently or invertibly. Indeed, otherwise, we could apply the splitting of Sect. 13.3.1 to T_i acting on $V^{I'_1\text{-nilp},I'_2\text{-inv}}$ and thereby refine (13.1) to get at least one more nonzero term, contradicting maximality.

13.3.5. Now take $V = A$ and $I = A$, where the elements $a \in A$ act on A by multiplication. These elements pairwise commute since A is commutative. Consider the corresonding decomposition of Sect. 13.3.4.

$$A \simeq \bigoplus_i J_i.$$

The vector subspaces $J_i \subset A$ are invariant under the multiplication by all elements of A — that is to say, they are ideals of A. Note also that $J_i \cdot J_j \subset J_i \cap J_j = 0$. Hence, setting $A_i := J_i$ we obtain a decomposition of A into a direct sum of algebras (the unit in each A_i is the projection of the unit in A onto the corresponding direct summand).

It remains to show that each A_i has the property stated in the theorem. With no restiction of generality, we can assume that $A = A_i$.

By assumption we can write A as a union of *sets* $A = A_1 \cup A_2$, such that all elements of A_1 act nilpotently, and all elements of A_2 act invertibly. Note that

$A_1 \subset A$ is the subset of all nilpotent elements of A. Certainly nilpotent elements of a commutative ring form an ideal. This is the sought-for ideal m. It remains to show that A/m is a field.

By assumption, any element $a \in A - m = A_2$ acts invertibly on A, and hence acts invertibly on the quotient A/m. Hence A/m has the property that multiplication by any nonzero element is an automorphism. This is equivalent to being a field.

□

14. Thursday, March 14

14.1. **Endomorphisms of fields.**

14.1.1. We will first show:

Lemma 14.1.2. *Let $L \supset K$ be a finite field extension. Then any endomorphism of L over K is an automorphism.*

Proof. Any ring homomorphism out of a field is automatically injective. But then the assertion follows from the fact that L is finite-dimensional over K (i.e., rank-nullity). □

14.1.3. We shall now generalize Lemma 14.1.2, which would also give a different proof in the finite case:

Proposition 14.1.4. *Let $L \supset K$ be an algebraic field extension. Then any endomorphism of L over K is an automorphism.*

Remark 14.1.5. Note that the assertion of Proposition 14.1.4 is false without the assumption that L is algebraic over K. For example, consider the endomorphism of $K(t)$ that sends $t \to t^2$, which is not surjective.

Proof of Proposition 14.1.4. Let ϕ denote our endomorphism. Again, it is automatically injective, and so we only need to show that it is surjective. That is, we need to show that every element $x \in L$ is in the image of ϕ.

Let $p(t) \in K[t]$ be the minimal polynomial of x over K. Let $x = x_1, \ldots, x_n$ be all the roots of p in L. It is clear that, for each i, $\phi(x_i) = x_j$ for some j (since the coefficients of the polynomial are fixed, so that the roots are permuted), so ϕ defines an endomorphism of the set $\{x_1, \ldots, x_n\}$. However, since ϕ is injective, this endomorphism is injective. Since the set in question is finite, it is also surjective by the pigeonhole principle.

□

14.2. **Algebraic closures.**

14.2.1. Recall that a field K is called algebraically closed if any the following equivalent conditions hold:

- Any polynomial $p(t) \in K[t]$ has a root in K;
- Any polynomial $p(t) \in K[t]$ factors into linear factors;
- Any irreducible polynomial in $K[t]$ has degree either 0 or 1.

14.2.2. Let K be a field. A field $\overline{K} \supset K$ is said to be *an* algebraic closure of K if both:

(i) $\overline{K} \supset K$ is algebraic,

(ii) and the field $\overline{K}$ is algebraically closed.

We will prove:

Theorem 14.2.3.

(a) *Any field admits an algebraic closure.*

(b) *Any two algebraic closures of a given field are isomorphic as field extensions.*

The proofs of these assertions will use Zorn's lemma — i.e., they will rely on the axiom of choice.

Remark 14.2.4. Working with the algebraic closure is a matter of convenience. All of our assertions with real content will be for finite field extensions, and instead of appealing to an algebraic closure, one can always use some "sufficiently large" finite extension (i.e., one containing all the roots of any polynomials under consideration). However, this would make the exposition cumbersome. So we'll instead rely on the blind choice hidden in Zorn's lemma.

14.2.5. We shall first prove point (b) of Theorem 14.2.3. To do this we will prove the following assertion, which will also be useful in the sequel:

Proposition 14.2.6. *Let $K \subset L$ be an algebraic extension, and let $K \subset M$ be a field extension with M algebraically closed. Then there exists a homomorphism of extensions $L \to M$.*

Let us recall the statement of Zorn's lemma:

Lemma 14.2.7. *Let I be a partially ordered set. Assume that for any linearly ordered (also called "totally ordered") subset $I' \subset I$ (i.e., one in which any two elements are comparable), there exists an upper bound of I' in I (i.e., an element $i_0 \in I$ such that $i_0 \geq i'$ for all $i' \in I'$). Then I contains a maximal element (i.e., an element i_1 such that $i \geq i_1 \Rightarrow i = i_1$ — i.e., there are no $i > i_1$).*

Intuitively one would just choose a random element and then take elements strictly larger than it and "induct". Of course this is not valid (the induction process may not terminate), and the axiom of choice in some sense allows for these infinitary induction arguments via Zorn's lemma.

Proof of Proposition 14.2.6. Consider the set I consisting of pairs (L', ϕ'), where $K \subset L' \subset L$ and ϕ' is a homomorphism of extensions $L' \to M$. We endow I with a partial ordering $(L'_1, \phi'_1) \leq (L'_2, \phi'_2)$ if $L'_1 \subset L'_2$ *and* $\phi'_2|_{L'_1} = \phi'_1$.

We claim that I satisfies the assumption of Zorn's lemma. Indeed, if $i \mapsto (L'_i, \phi'_i)$ is a nested family of field extensions with compatible maps to M, its upper bound is provided by $\cup_i L'_i$, and the 'union' of the ϕ_i.

By Zorn's lemma, there exists a maximal element $(L', \phi') \in I$. We claim that $L' = L$.

Suppose not. We regard M as a field extension of L' via ϕ'. Let $x \in L - L'$. Since x is algebraic over K, it is algebraic over L'. Let $p(t) \in L'[t]$ be the minimal polynomial of x over L'. Consider the field $L'_1 = L'(x)$ generated by x. We

claim that the homomorphism $\phi' : L' \to M$ can be extended to a homomorphism $\phi'_1 : L'_1 \to M$. (This would contradict the maximality of L'.)

Indeed, $L'_1 = L'_p$ and the datum of ϕ'_1 is equivalent to that of a root of $p(t)$ (viewed as a polynomial with coefficients in M via ϕ') in M. Such a root exists by assumption: M is algebraically closed.

□

Proof of Theorem 14.2.3(b). Let $\overline{K}_1 \supset K \subset \overline{K}_2$ be two algebraic closures. By Proposition 14.2.6 there exist (completely noncanonical) homomorphisms of extensions

$$\phi : \overline{K}_1 \leftrightarrows \overline{K}_2 : \psi.$$

By Proposition 14.1.4, the composition $\phi \circ \psi$ is an *automorphism* of $\overline{K}_2$, and the composition $\psi \circ \phi$ is an *automorphism* of $\overline{K}_1$.

Hence ϕ and ψ are both isomorphisms.

□

14.2.8. *Proof of Theorem 14.2.3(a).* We will use the following assertion, whose proof uses Zorn's lemma:

Lemma 14.2.9. *For any field K there exists an algebraic extension $K \subset K'$, such that any polynomial in K admits a root in K'.*

(In fact K' is actually already algebraically closed, but we won't need this fact for our construction. The point is that iteratively applying this lemma secretly does nothing after the first step.)

Define the fields K_i inductively with $K_0 = K$ and $K_{i+1} = K'_i$, where $K_i \subset K'_i$ is as in Lemma 14.2.9. Set

$$\overline{K} := \bigcup_i K_i.$$

We claim that $\overline{K}$ is an algebraic closure of K. First, each K_i, being a successive extension of algebraic extensions of K, is itself algebraic. Hence, $\overline{K}$ is algebraic over K, since any element of $\overline{K}$ belongs to some K_i.

Next, we claim that any polynomial $p(t) \in \overline{K}[t]$ admits a root in $\overline{K}$. Indeed, since every polynomial has only finitely many coefficients, it belongs to $K_i[t]$ for some i. Hence, it admits a root in K_{i+1}, by the construction of K_{i+1}.

□

Note that the lemma is actually a reduction: an algebraic closure has to be algebraically closed itself, but now we need only produce a field in which every polynomial *of the base* has a root. This we can reasonably do by "induction" — i.e., Zorn's lemma. (Do you see why it would be hard to apply Zorn without such a reduction? For example, it is very easy to produce a sequence of integers coprime to a fixed given integer, but it is much harder to write down a sequence of integers coprime to all smaller integers (i.e., the primes). The point is that the latter condition is significantly harder to check.)

Anyway, let's now prove the lemma. The point will be that we will just add on roots inductively, and Zorn's lemma will tell us that this works.

Proof of Lemma 14.2.9. Let I be the set of tuples $(A, L, \{x_p\}_{p \in A})$ for $A \subseteq K[t]$ a set of polynomials, L a field in which all elements of A have a root, and x_p a choice

of root of p in L (so that $p(x_p) = 0$ in L), with the added condition that the x_p generate L over K (i.e., $K(\{x_p\}) = L$).

Order I via setting $(A, L, \{x_p\}) \leq (A', L', \{x'_q\})$ if $A \subseteq A'$, and there is a map (embedding) $L \to L'$ taking $x_p \mapsto x'_p$ for every $p \in A$. Note that this map, if it exists, is automatically unique, since the x_p generate L over K.

Equipped with this uniqueness statement, if we proceed as we did above Zorn's lemma then applies to I. (Do this for practice with Zorn's lemma!) Hence there is a maximal element $(A, L, \{x_p\}) \in I$. The claim is that $K' := L$ is as claimed.

Let $P(t)$ be an irreducible polynomial in $K[t]$. Suppose for the sake of contradiction that $P(t)$ does not admit a root in L. Let $Q(t) \in L[t]$ be any irreducible factor of $P(t)$. Let $A' := A \sqcup \{P(t)\}$. Let $L' := L[t]/(Q(t))$. Let $x'_p := x_p$ for $p \in A$, and let x'_P be the image of t in L'.

Then certainly $A \subset A'$, and the evident map $L \to L[t]/(Q(t)) = L'$ tautologically takes x_p to x'_p for each $p \in A$. Hence $(A, L, \{x_p\}) \leq (A', L', \{x'_p\})$. But $A \neq A'$. This contradicts the maximality of $(A, L, \{x_p\})$. Thus the claim.

□

14.3. **Normal extensions.**

14.3.1. Let $K \subset L$ be an algebraic field extension.

Proposition 14.3.2. *The following conditions are equivalent:*

(1) *If an irreducible polynomial $p(t) \in K[t]$ has a root in L, then it factors completely in L.*[3]

(2) *L is generated over K by elements x such that, for each x, the minimal polynomial of x over K factors completely in L.*

(3) *If $K \subset L'$ is some other field extension, and $\phi, \psi : L \to L'$ are two homomorphisms, then* $\mathrm{Im}(\phi) = \mathrm{Im}(\psi)$.

(4) *Same as* (3) *but replacing the condition on* every L' *with the same for* one *algebraic closure $\overline{K}$ of K.*

Definition 14.3.3. *Extensions satisfying the equivalent conditions of Proposition 14.3.2 are called* normal.

14.3.4. *Proof of Proposition 14.3.2.* The implications (1) ⇒ (2) and (3) ⇒ (4) are tautological.

Let us prove that (2) implies (3). Let $\phi, \psi : L \to L'$ be two homomorphisms. Let x be one of the guaranteed generators of L over K with the property that its minimal polynomial over K factors completely in L. It is then enough to show that $\phi(x) \in \mathrm{Im}(\psi)$.

Let $x = x_1, \ldots, x_n$ be all the roots of $p(t)$ in L, so that

$$p(t) = \prod_i (t - x_i)^{k_i}$$

for some $k_i \in \mathbb{Z}^+$.

[3]This means, that when considered as an element of $L[t]$, it can be written as a product of linear factors.

Viewing $p(t)$ as an element of $L'[t]$, we also have

$$\prod_i (t - \phi(x_i))^{k_i} = p(t) = \prod_i (t - \psi(x_i))^{k_i}.$$

This shows in particular that the subsets

$$\{\phi(x_1), \ldots, \phi(x_n)\} \text{ and } \{\psi(x_1), \ldots, \psi(x_n)\}$$

of L' coincide. Hence $\phi(x_1) = \psi(x_i)$ for some i.

Next, let us prove that (4) implies (1). Let $p(t)$ be an irreducible polynomial which has a root $x \in L$. Choose an embedding $\phi : L \hookrightarrow \overline{K}$, which exists by Proposition 14.2.6. Let $x_1, \ldots, x_n$ be the roots of $p(t)$ in $\overline{K}(t)$, and without loss of generality number so that $x_1 = \phi(x)$. We need to show that $x_i \in \mathrm{Im}(\phi)$ for all i.

For a given i, consider the embeddings of extensions $L_p \to L$ via $x_{univ} \mapsto x$, and $L_p \to \overline{K}$ via $x_{univ} \mapsto x_i$. By Proposition 14.2.6, we can extend $L_p \to \overline{K}$ to a map $\psi : L \to \overline{K}$. By the assumption in (4), we have $\mathrm{Im}(\psi) = \mathrm{Im}(\phi)$. Hence $x_i \in \mathrm{Im}(\phi)$, as required.

□

Week 7, Problem 6. *Show that normality of L is also equivalent to the following two conditions:*

(a) *For every embedding of extensions $L \subset L'$, if an irreducible polynomial $p(t) \in K[t]$ has a root in L, then any of its roots in L' belong to L.*

(b) *Same as* (a)*, but for L' being some fixed algebraic closure of K.*

14.3.5. Here is an example of a non-normal extension. Let $a \in K$ be an element which is not a cube (e.g., $2 \in \mathbb{Q}$). Consider the polynomial $p(t) = t^3 - a$. It is irreducible over K. (Indeed, if it were reducible, $p(t)$ would contain a linear factor, contradicting the fact that $p(t)$ doesn't have roots in K.) Consider the corresponding field $L_p := K[t]/(p(t))$.

Assume now that K does *not* contain a primitive third root of unity (e.g., $K = \mathbb{Q}$ does not, since $x^3 = 1$ in $\mathbb{Q}$ implies $x = 1$). We claim that, in this case, L_p is not normal.

Namely, suppose it is normal. Then p splits in L_p (i.e., it factors into linear factors). Let $x_{univ} = x_1, x_2$, and x_3 be the three roots of p in L_p. Note that $\omega := \frac{x_1}{x_2}$ is a third root of unity distinct from 1. Then L_p contains the subfield $K(\omega)$. But the minimal polynomial of ω is $t^2 + t + 1$ (since $t^3 - 1 = (t-1)(t^2 + t + 1)$ and K does not contain ω). Hence $K(\omega)$ is a degree 2 extension of K. But L_p is a degree 3 extension of K. We have already seen that

$$\deg(L_p/K(\omega)) \deg(K(\omega)/K) = \deg(L_p/K),$$

a contradiction since 2 does not divide 3.

It is worth noting that, upon adding the third roots of unity, the extension becomes normal. As we have seen the field must have third roots of unity if it is to be normal, so this is the minimal such field. Such a thing is called the *normal closure* of the field L_p. We will see that over $\mathbb{Q}$ this field is Galois (which we will define!) with Galois group S_3.

15. Tuesday, March 26

15.1. **Another criterion for normality.**

15.1.1. Let $K \subset L$ be a finite field extension. Consider the tensor product

$$A := L \underset{K}{\otimes} L$$

as an L-algebra via the map

$$\psi : L \to L \underset{K}{\otimes} L, \quad x \mapsto x \otimes 1.$$

We will also consider a *different* map of K-algebras

$$\phi : L \to L \underset{K}{\otimes} L, \quad x \mapsto 1 \otimes x.$$

Let us apply to A the decomposition of Theorem 13.2.5,

$$A \simeq \bigoplus_{i \in I} A_i.$$

Let L_i denote the corresponding quotient A_i/m_i. Let π_i denote the resulting map

$$L \underset{K}{\otimes} L \to L_i,$$

and let $\psi_i : L \to L_i$ denote the composition

$$L \xrightarrow{\psi} L \underset{K}{\otimes} L \xrightarrow{\pi_i} L_i.$$

Let $\phi_i : L \to L_i$ denote the composition

$$L \xrightarrow{\phi} L \underset{K}{\otimes} L \xrightarrow{\pi_i} L_i.$$

For example, if L is generated by one element x over K, let $p(t)$ be the minimal polynomial of x over K. Then $L \simeq K[t]/(p(t))$, and $A = L[t]/(p(t))$. Factor $p(t) = \prod_i q_i(t)^{k_i}$ into irreducibles in $L[t]$. Then (we will see all these isomorphisms soon, but they are certainly plausible)

$$L \underset{K}{\otimes} L \simeq L[t]/(p(t)) \simeq \bigoplus_i L[t]/(q_i(t)^{k_i}).$$

Also, $m_i \subset A_i = L[t]/(q_i(t)^{k_i})$ is just $m_i = (q_i(t))$, so the quotient is $L_i = A_i/m_i \simeq L[t]/(q_i(t))$. This is the example to keep in mind throughout.

15.1.2. We are going to prove:

Theorem 15.1.3. *The extension L/K is normal if and only if each of the maps $\phi_i, \psi_i : L \to L_i$ is an isomorphism.*

(In our example, this says that each q_i is in fact linear — i.e., $L[t]/(q_i(t)) \simeq L$. Hence we see that this precisely tells us that $p(t)$ splits into (possibly repeated) linear factors in L.)

Proof. Let us first prove the "only if" direction. We need to show that the map ψ_i is surjective. Note that the map π_i is surjective. Hence, any element of L_i can be written as a sum of elements of the form

$$\pi_i(x' \otimes x'') = \psi_i(x') \cdot \phi_i(x'').$$

Since L/K was assumed normal, $\mathrm{Im}(\phi_i) = \mathrm{Im}(\psi_i)$. Hence $\phi_i(x'') = \psi_i(x''')$ for some $x''' \in L$. Setting $x = x' \cdot x'''$, we obtain

$$\pi_i(x' \otimes x'') = \psi_i(x).$$

So the image of ψ_i spans L_i as a K-vector space. Since ψ_i is K-linear, it is surjective.

Let us now prove the "if" direction. Let α, β be two K-homomorphisms $L \to M$, where M is some field. We need to show that, say, $\mathrm{Im}(\beta) \subset \mathrm{Im}(\alpha)$.

Define a map of rings

$$\gamma : L \underset{K}{\otimes} L \to M, \quad \gamma(x' \otimes x'') = \alpha(x') \cdot \beta(x'').$$

As in Step 2 in the proof of Theorem 13.2.2, the map γ factors as

$$L \underset{K}{\otimes} L \xrightarrow{\pi_i} L_i \xrightarrow{\delta} M$$

for some index i. By definitions

$$\alpha = \delta \circ \pi_i \circ \psi = \delta \circ \psi_i \text{ and } \beta = \delta \circ \pi_i \circ \phi = \delta \circ \phi_i.$$

Hence it suffices to show that

$$\mathrm{Im}(\phi_i) \subset \mathrm{Im}(\psi_i).$$

However, this is automatic since the map ψ_i is surjective by hypothesis.

□

Of course, if $\psi_i : L \to L_i$ is an isomorphism, then so is ϕ_i since it is automatically an injection and the dimensions agree.

15.2. **Separable polynomials.** In this subsection all fields will be of characteristic $\ell \geq 0$.

15.2.1. For a polynomial $p(t) \in K[t]$ we define its derivative as follows: if

$$p(t) =: \sum_{i=0}^{n} a_i t^i = a_0 + \cdots + a_n t^n,$$

then

$$p'(t) := \sum_{i=1}^{n} i a_i t^{i-1} = a_1 + \cdots + n a_n t^{n-1}.$$

This is of course the usual derivative, except we can't just think of the polynomial as a function of a real or complex variable since K may not have anything to do with $\mathbb{R}$ or $\mathbb{C}$.

Definition 15.2.2. *We shall say that an irreducible polynomial $p(t)$ is* separable *if $p'(t) \neq 0$.*

Note that, if $p(t) = \sum_i a_i t^i$, then $p(t)$ is *inseparable* if and only if

$$a_i \neq 0 \Rightarrow p \,|\, i.$$

Note that, in characteristic zero, *every* polynomial is automatically separable.

Hence, if $p(t)$ is inseparable, then $\ell > 0$ and there exists a polynomial $q(t) \in K[t]$ such that

$$p(t) = q(t^\ell).$$

Proposition 15.2.3. *An irreducible polynomial $p(t) \in K[t]$ is separable if and only if it does not have multiple roots in $\overline{K}$.*

Proof. Consider $\gcd(p(t), p'(t))$. Since $p(t)$ is irreducible, by considering degrees it is separable if and only if $\gcd(p(t), p'(t)) = 1$.

Lemma 15.2.4. *Let $K \hookrightarrow L$ be a field extension. Then for $q_1, q_2 \in K[t]$, their* gcd *as polynomials with coefficients in K equals their* gcd *as polynomials with coefficients in L.*

Proof. Do it yourself. (Hint: let d be the greatest common divisor of q_1, q_2. Then there exist $a_1, a_2 \in K[t]$ for which $a_1 q_1 + a_2 q_2 = d$.) □

Hence, we obtain that $p(t)$ is separable if and only if $\gcd(p(t), p'(t)) = 1$ as polynomials with coefficients in $\overline{K}$. Now, the assertion of the proposition follows from the next (obvious) lemma:

Lemma 15.2.5. *Let $\prod_{i \in I} (t - a_i)^{n_i} \in L[t]$ be a polynomial over a field L. Then $\gcd(p(t), p'(t)) = 1$ if and only if all $n_i = 1$.*

□

15.2.6. *An example.* Here is a typical example of an inseparable polynomial. Take $\ell > 0$. Let $a \in K$ be such that a does not admit a ℓ-th root in K (if it exists — otherwise K is called *perfect*. That is, K is perfect if $\ell = 0$ or $\ell > 0$ and every element of K admits an ℓ-th root.). Consider the polynomial

$$p(t) := t^\ell - a.$$

Clearly $p'(t) = 0$ in $K[t]$. We claim that $p(t)$ is irreducible. Indeed, let b be a root of p in $\overline{K}$. Then, as a polynomial with coefficients in $\overline{K}$, we have

$$p(t) = (t - b)^\ell.$$

Let $q(t)$ be a monic factor of $p(t)$. Then, when viewed as a polynomial with coefficients in $\overline{K}$, we have $q(t) = (t - b)^n$ for some $n \leq \ell$. We claim that $n = \ell$ or $n = 0$. Indeed, otherwise $(t - b)^n = t^n - nbt^{n-1} + \cdots$, and $n \neq 0$ (since $0 < n < \ell$) in K implies that this cannot lie in K, since otherwise $nb \in K$, whence $b \in K$, a contradiction.

15.2.7. In what follows we will also use the following:

Definition 15.2.8. *Let $L \supset K$ be a field extension and let $x \in L$ be an element. We shall say that x is* separable *over K if its minimal polynomial over K is separable.*

15.2.9. *Separable field extensions.* Let $L \supset K$ be a finite extension.

Definition 15.2.10. *We shall say that L/K is separable if the $\overline{K}$-algebra $\overline{K} \underset{K}{\otimes} L$ has no nilpotent elements.*

(Note that this does not depend on the choice of algebraic closure $\overline{K}$.)

It will turn out that this is equivalent to saying that L/K is separable if every element $x \in L$ has separable minimal polynomial over K. (This is the usual definition.)

For example, let's look at our old example of $L = K[t]/(p(t))$, with $p(t)$ an irreducible polynomial in $K[t]$. Factor

$$p(t) = \prod_i (t - a_i)^{k_i}$$

in $\overline{K}[t]$. Then

$$\overline{K} \underset{K}{\otimes} L \simeq \overline{K}[t]/(p(t)) \simeq \bigoplus_i \overline{K}[t]/((t - a_i)^{k_i})$$

(do you see why?). Now if any $k_i > 1$, then $(0, \ldots, t - a_i, \ldots, 0)$ is nilpotent (consider its k_i-th power). Otherwise, if each $k_i = 1$, then this is isomorphic to $\bigoplus_i \overline{K}$, which has no nilpotents (why?).

We are going to prove:

Proposition 15.2.11. *Let $K \subset L \subset M$ be finite field extensions. Then M/K is separable if and only if M/L and L/K are separable.*

Had we called an extension separable if every element had a separable minimal polynomial, one direction (the forward direction) would be tautological (do you see why?). But the reverse would be hard. The advantage of this definition is that it makes both directions easy.

Proof. We first prove the "only if" direction. Let M/K be separable.

Let us show that L/K is separable. Consider the map

$$\overline{K} \underset{K}{\otimes} L \to \overline{K} \underset{K}{\otimes} M.$$

It is injective, because the operation of tensoring vector spaces over K preserves injectivity, and $L \to M$ was injective. Hence if $\overline{K} \underset{K}{\otimes} M$ has no nilpotents, the same is certainly true for $\overline{K} \underset{K}{\otimes} L$.

Let us now show that M/L is separable. Let us extend the embedding $K \hookrightarrow \overline{K}$ to $L \hookrightarrow \overline{K}$ (this is possible by Proposition 14.2.6). This gives rise to a surjection of $\overline{K}$-algebras

$$\overline{K} \underset{K}{\otimes} M \to \overline{K} \underset{L}{\otimes} M.$$

(Namely, we quotient out by the relations $(x\alpha) \otimes \beta = \alpha \otimes (x\beta)$ for $x \in K$ on the left, and we quotient out by the same relations for $x \in L \supset K$ on the right.)

By assumption,

$$\overline{K} \underset{K}{\otimes} M =: A \simeq \bigoplus_i A_i =: \bigoplus_i \overline{K}_i,$$

where $\overline{K}_i$ are fields (since each $m_i = 0$). Note that, in fact, since each $\overline{K}$ is a finite extension of $\overline{K}$ (which is algebraically closed), $\overline{K}_i = \overline{K}$. Now the required assertion follows from the next lemma:

Lemma 15.2.12. *Let R be a ring isomorphic to a direct sum of finitely many fields. Then any ideal in R is the direct sum of a subset of these fields.*

Week 8, Problem 1. *Prove Lemma 15.2.12.*

Indeed, with the lemma, we have $\overline{K} \underset{L}{\otimes} M \simeq (\overline{K} \underset{K}{\otimes} M)/\ker$ (where ker is the kernel of the surjection $\overline{K} \underset{K}{\otimes} M \to \overline{K} \underset{L}{\otimes} M$). Since the kernel is an ideal, by the lemma it is a direct sum of a subset of these fields, and so the quotient is direct sum of the rest of the fields. In particular $\overline{K} \underset{L}{\otimes} M$ is also a direct sum of fields! Hence it has no nilpotents.

We now turn to the "if" direction. Write

$$\overline{K} \underset{K}{\otimes} M \simeq (\overline{K} \underset{K}{\otimes} L) \underset{L}{\otimes} M,$$

where we view $\overline{K} \underset{K}{\otimes} L$ as an L-algebra via the map

$$\phi : L \to \overline{K} \underset{K}{\otimes} L, \quad x \mapsto 1 \otimes x.$$

By assumption,

$$\overline{K} \underset{K}{\otimes} L =: A' \simeq \bigoplus_i A'_i \simeq \bigoplus_i \overline{K}_i,$$

where $\overline{K}_i$ are fields, and again each $\overline{K}_i \simeq \overline{K}$. Thus,

$$\overline{K} \underset{K}{\otimes} M \simeq \bigoplus_i \overline{K}_i \underset{L}{\otimes} M,$$

where $\overline{K}_i \simeq \overline{K}$ is an L-algebra via the map $\phi_i = \pi_i \circ \phi$. It suffices to show that each $\overline{K}_i \underset{L}{\otimes} M$ has no nilpotent elements. But this is immediate: the ϕ_i are just different embeddings of L into $\overline{K}$ — i.e., maps making $\overline{K}$ into an algebraic closure of L. But since M was assumed separable over L the result follows since each $\overline{K}_i \underset{L}{\otimes} M$ has no nilpotents.

□

15.3. **Separability of extensions versus separability of elements.**

15.3.1. Let $p(t) \in K[t]$ be an irreducible polynomial. We claim:

Proposition 15.3.2. *The polynomial $p(t)$ is separable if and only the extension $L_p = K[t]/p(t)$ is separable.*

For the proof we will need the following assertion:

Week 8, Problem 2. *Let $\phi : R_1 \to R_2$ be a homomorphism of commutative rings, and let $q(t)$ be an element of $R_1[t]$. Construct a canonical isomorphism of R_2-algebras*

$$R_2 \underset{R_1}{\otimes} R_1[t]/(q(t)) \simeq R_2[t]/(\phi(p(t))).$$

Proof of Proposition 15.3.2. Consider the $\overline{K}$-algebra

$$\overline{K} \underset{K}{\otimes} L_p.$$

By Problem 2, it is isomorphic to

$$\overline{K}[t]/(p(t)),$$

where $p(t)$ is viewed as a polynomial with coefficients in $\overline{K}$.

Write $p(t) = \prod_i (t-a_i)^{n_i}$, where $a_i \neq a_j$. The Chinese Remainder Theorem says that

$$\overline{K}[t]/(p(t)) \simeq \bigoplus_i \overline{K}[t]/(t-a_i)^{n_i}.$$

From here (as we detailed above) it is clear that $\overline{K}[t]/(p(t))$ has no nilpotent elements if and only if all $n_i = 1$.

□

15.3.3. We are going to prove:

Proposition 15.3.4. *Let $L \supset K$ be a finite field extension. Then the following conditions are equivalent:*

(a) *Every element of L is separable over K;*

(b) *L is generated over K by separable elements;*

(c) *L/K is a separable field extension.*

Proof. The implication (a) $\Rightarrow$ (b) is tautological. Let us show that (b) implies (c). Let $x_1, \ldots, x_n$ be separable elements that generate L over K. Set $L_i = K(x_1, \ldots, x_i)$. By Proposition 15.2.11, it suffices to show that L_i is separable over L_{i-1}.

Let $p_i(t) \in K[t]$ be the minimal polynomial of x_i over K, and let $q_i(t) \in L_{i-1}[t]$ be the minimal polynomial of x over L_{i-1}. Immediately we see that $q_i(t) | p(t)$. Hence, if $p(t)$ has no multiple roots in $\overline{K}$, the same is true for $q_i(t)$. Hence we obtain that x is separable over L_{i-1}. By Proposition 15.3.2, we see that L_i is separable over L_{i-1}, as desired.

Finally, let us prove that (c) implies (a). For $x \in L$ consider the subextension $K(x) \subset L$. It is separable by Proposition 15.2.11. Hence, x is separable by Proposition 15.3.2.

□

Week 8, Problem 3. *Show that a finite field extension L/K is separable if and only if the inequality $|\mathrm{Hom}_{K\text{-Alg}}(L, \overline{K})| \leq \deg(L/K)$ is an equality.*

Week 8, Problem 4. *Let $L \supset K$ be a field extension. Show that set of elements of L that are separable over K form a subfield.*

15.3.5. A field of characteristic ℓ is said to be *perfect* if the map

$$x \mapsto x^\ell : K \to K$$

(called the *Frobenius automorphism*, or *Frobenius* for short) is surjective.

Week 8, Problem 5. *Show that the following conditions are equivalent: (a) K is perfect; (b) any irreducible polynomial in $K[t]$ is separable; (c) any finite field extension of K is separable; (d) any algebraic field extension of K consists of separable elements.*

15.3.6. Let $L \supset K$ be an algebraic field extension. We let L^s be the subset of L consisting of elements separable over K. According to Problem 4, L^s is a subfield.

Week 8, Problem 6. *Show that if L/K is normal, then so is L^s/K.*

Definition 15.3.7. *We shall say that an algebraic field extension $K \subset L$ is* purely inseparable *if $L^s = K$.*

Week 8, Problem 7. *Show that for an algebraic field extension $K \subset L$, the extension $L^s \subset L$ is purely inseparable.*

Hence any algebraic extension can be broken up into a tower of a separable extension $L^s \supset K$ and a purely inseparable extension $L \supset L^s$.

16. Thursday, March 28

16.1. Galois extensions.

16.1.1. Let $L \supset K$ be a finite field extension.

Definition 16.1.2. *We shall say that L/K is* Galois *if it is both normal and separable.*

Lemma 16.1.3. *Let $K \subset L' \subset L$ be a tower of extensions. If L/K is Galois, then so is L/L'.*

However, L'/K is ***not*** necessarily Galois. This will turn out to be equivalent to the fact that a subgroup of a group need not be normal in general.

Proof. We have seen that L/L' is separable in Proposition 15.2.11. It remains to see that L/L' is normal. But this follows from Proposition 14.3.2(3). □

Remark 16.1.4. Note that the converse is not true: the composition of normal extensions doesn't have to be normal. (Example: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$.) Nor (again) is it true that L'/K is normal in general. (Example: $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$, with ω a primitive cube root of unity.)

Proposition 16.1.5. *A finite extension L/K is Galois if and only if in the decomposition*

$$L \underset{K}{\otimes} L \simeq \bigoplus_i A_i,$$

each $A_i = L_i$ is a field, and each map

$$\psi_i : L \xrightarrow{\psi} L \underset{K}{\otimes} L \xrightarrow{\pi_i} L_i$$

is an isomorphism.

Proof. Assume that L/K is Galois. By Theorem 15.1.3, we only need to show that $L \underset{K}{\otimes} L$ is nilpotent-free. However, the map

$$L \underset{K}{\otimes} L \to \overline{K} \underset{K}{\otimes} L$$

is an injection, and the assertion follows from the separability of L/K.

Vice versa, suppose that each $A_i = L_i$ is a field, and each ψ_i is an isomorphism. The fact that L/K is normal then follows from Theorem 15.1.3. To show that L/K is separable, we write

$$\overline{K} \underset{K}{\otimes} L \simeq \overline{K} \underset{L}{\otimes} (L \underset{K}{\otimes} L) \simeq \bigoplus_i \overline{K} \underset{L}{\otimes} L_i.$$

Now, each $\overline{K} \underset{L}{\otimes} L_i \simeq \overline{K} \underset{L}{\otimes} L \simeq \overline{K}$ by assumption. Hence $\overline{K} \underset{K}{\otimes} L$ is a direct sum of fields, whence nilpotent-free.

□

Combining Proposition 16.1.5 with Corollary 13.2.9, we obtain:

Corollary 16.1.6. *A finite extension L/K is Galois if and only if the inequality*

$$|\operatorname{End}_{K\text{-Alg}}(L)| \leq \deg(L/K)$$

is an equality.

16.1.7. Let L/K be a Galois extension. Recall that every element of $\operatorname{End}_{K\text{-Alg}}(L)$ is an automorphism.

We define the *Galois group* of L over K, denoted $\operatorname{Gal}(L/K)$ to be $\operatorname{Aut}_{K\text{-Alg}}(L)$.

By Corollary 16.1.6, we have

$$|\operatorname{Gal}(L/K)| = \deg(L/K).$$

16.2. **The tensor product picture.**

16.2.1. Let L/K be a Galois extension. Consider again the tensor product

$$A := L \underset{K}{\otimes} L,$$

equipped with the maps $\phi, \psi : L \to A$,

$$\phi(x) = 1 \otimes x, \quad \psi(x) = x \otimes 1.$$

By Proposition 16.1.5, we have a canonical isomorphism

$$A \simeq \bigoplus_{i \in I} L,$$

where for every i, the map ψ_i

$$L \xrightarrow{\psi} A \xrightarrow{\pi_i} L$$

is the identity map.

Recall that ϕ_i denotes the composed map

$$L \xrightarrow{\phi} A \xrightarrow{\pi_i} L.$$

16.2.2. Note now that by [Week 7, Problem 5], the set I is in a canonical bijection with the set

$$\mathrm{Gal}(L/K) = \mathrm{Aut}_{K\text{-Alg}}(L) = \mathrm{Hom}_{K\text{-Alg}}(L, L) \simeq \mathrm{Hom}_{L\text{-Alg}}(A, L).$$

Namely, to an element $i \in I$ we attach the map $\phi_i : L \to L$.

So, henceforth, we will rewrite

$$L \underset{K}{\otimes} L \simeq \bigoplus_{g \in \mathrm{Gal}(L/K)} L \simeq \mathrm{Fun}(\mathrm{Gal}(L/K), L), \tag{16.1}$$

where for every $g \in \mathrm{Gal}(L/K)$, the map ψ_g

$$L \xrightarrow{\psi} A \xrightarrow{\pi_g} L$$

is the identity map, and the map ϕ_g

$$L \xrightarrow{\phi} A \xrightarrow{\pi_g} L$$

is given by the *action of the element* $g \in \mathrm{Aut}_{K\text{-Alg}}(L)$ *on* L.

16.2.3. Note that the ring $L \underset{K}{\otimes} L$ comes equipped with an action of the group $\mathrm{Gal}(L/K) \times \mathrm{Gal}(L/K)$, where an element $(g_1, g_2) \in \mathrm{Gal}(L/K) \times \mathrm{Gal}(L/K)$ acts by

$$(g_1, g_2) \cdot (x_1, x_2) = (g_1 \cdot x_1, g_2 \cdot x_2).$$

Consider the action of $\mathrm{Gal}(L/K) \times \mathrm{Gal}(L/K)$ on $\mathrm{Fun}(\mathrm{Gal}(L/K), L)$ arising from isomorphism (16.1).

Week 8, Problem 8. *Show that the above action is given by*

$$((g_1, g_2) \cdot f)(g) = g_1 \cdot f(g_1^{-1} g g_2),$$

where the "outer" g_1 *corresponds to the action of* $g_1 \in \mathrm{Gal}(L/K)$ *on the element* $f(g_1^{-1} g g_2) \in L$.

16.3. **The fundamental theorem of Galois theory.** In this subsection, $L \supset K$ will be a Galois extension. Denote $G := \mathrm{Gal}(L/K)$.

16.3.1. Let $K \subset L' \subset L$ be a subextension. Define the subgroup

$$\mathrm{Stab}(L') \subset G$$

to consist of those $g \in G$ such that $g(x) = x$ for all $x \in L'$. (This is called the *corresponding subgroup* to the subextension $L' \subset L$.)

It is clear that $\mathrm{Stab}(L')$ identifies with $\mathrm{Aut}_{L'\text{-Alg}}(L)$. Since L/L' is Galois, we obtain that

$$\mathrm{Stab}(L') \simeq \mathrm{Gal}(L/L') =: G'.$$

In particular, we obtain:

Lemma 16.3.2. $|G'| = \deg(L/L')$.

16.3.3. Let $H \subset G$ be a subgroup. Define $L^H \subset L$, the *fixed field of* H, to be the subset of those elements $x \in L$ such that $h(x) = x$ for all $h \in H$. Clearly L^H/K is a subextension of L/K.

Proposition 16.3.4. $\deg(L/L^H) = |H|$.

Proof. It suffices to show that

$$\deg(L^H/K) = |G/H|.$$

By definition, $\deg(L^H/K) = \dim_K(L^H)$. But

$$\dim_K(L^H) = \dim_L(L \underset{K}{\otimes} L^H).$$

Now, for any group H acting on a vector space V and a finite-dimensional W, we have

$$W \otimes V^H \simeq (W \otimes V)^H,$$

where on the right-hand side H acts only on the second factor. (Proof: decompose W as a direct sum of copies of K.)

To summarize, we obtain

$$\deg(L^H/K) = \dim_L \left(L \underset{K}{\otimes} L^H \right).$$

We will show that $L \underset{K}{\otimes} L^H$ is isomorphic as an L-vector space to $\mathrm{Fun}(G/H, L)$.

Recall the setting of Problem 8. We will regard $L \underset{K}{\otimes} L$ as equipped with the action of G on the right factor of L. Now the required assertion is manifest from that of Problem 8.

□

16.3.5. Consider the sets

$$\{\text{subextensions of } K \subset L\} \text{ and } \{\text{subgroups of } G\}.$$

Consider the maps

$$\{\text{subextensions of } K \subset L\} \to \{\text{subgroups of } G\}, \quad L' \rightsquigarrow \mathrm{Stab}(L')$$

and

$$\{\text{subgroups of } G\} \to \{\text{subextensions of } K \subset L\}, \quad H \rightsquigarrow L^H.$$

The fundamental theorem of Galois theory says:

Theorem 16.3.6. *The above maps are inverse bijections.*

Proof. Clearly, for a subextension L', we have

$$L' \subset L^{\mathrm{Stab}(L')}.$$

However, by Proposition 16.3.4 and Lemma 16.3.2, we have

$$\deg(L/L') = |\mathrm{Stab}(L')| = \deg(L/L^{\mathrm{Stab}}(L')).$$

Hence the above inclusion is an equality.

For a subgroup $H \subset G$, we have

$$H \subset \mathrm{Stab}(L^H).$$

However, again, by Proposition 16.3.4 and Lemma 16.3.2, we have

$$|H| = \deg(L/L^H) = |\operatorname{Stab}(L^H)|,$$

so the inclusion is an equality.

□

16.4. **Normality of groups versus normality of extensions.** We continue to assume that L/K is a Galois extension with Galois group G.

16.4.1. Let $H \subset G$ be a subgroup, and let $g \in G$ be an element. We have:

Lemma 16.4.2. $g(L^H) = L^{gHg^{-1}}$.

Proof. Obvious. □

Similarly, for a subextension $L' \subset L$ and $g \in G$ we have:

Lemma 16.4.3. $\operatorname{Stab}(g(L')) = g \operatorname{Stab}(L')g^{-1}$.

16.4.4. We now claim:

Proposition 16.4.5. *A subextension L'/K of L/K is normal if and only if the subgroup $\operatorname{Stab}(L')$ is normal a subgroup of G. If this is the case, $\operatorname{Gal}(L'/K)$ is canonically isomorphic to the quotient $G/\operatorname{Stab}(L')$.*

Proof. Suppose that L'/K is normal. Then for any $g \in G$ we have $g(L') = L'$ (see Proposition 14.3.2(3)). Hence, $\operatorname{Stab}(L')$ is normal by Lemma 16.4.3 and the fundamental theorem (Theorem 16.3.6).

Vice versa, assume that $H \subset G$ is normal, and let $L' = L^H$. First, we claim that any $g \in G$ maps L' to itself. Indeed, this follows from Lemma 16.4.2.

Hence, we obtain that the group G maps to $\operatorname{Aut}_{K\text{-alg}}(L')$. Furthermore, the subgroup $H \subset G$ lies in the kernel of this map. Hence we obtain a homomorphism

$$G/H \to \operatorname{Aut}_{K\text{-alg}}(L').$$

We claim that this homomorphism is injective. Indeed, if $g \in G$ acts trivially on L^H, then it belongs to $\operatorname{Stab}(L^H) = H$, where we have again used Theorem 16.3.6.

Thus, we have a string of inequalities

$$|G/H| \leq |\operatorname{Aut}_{K\text{-alg}}(L')| \leq \deg(L'/K) = |G/H|.$$

Hence all of the above inequalities are equalities. In particular,

$$|\operatorname{Aut}_{K\text{-alg}}(L')| = \deg(L'/K),$$

so L'/K is Galois by Corollary 16.1.6. Furthermore,

$$G/H \to \operatorname{Aut}_{K\text{-alg}}(L')$$

is an isomorphism, as contended.

□

Week 8, Problem 9. *Let $L' \subset L$ be an arbitrary subextension. Let $H := \operatorname{Stab}(L')$. Let $N(H)$ be the normalizer of H in G (i.e., the set of all elements $g \in G$ such that $gHg^{-1} = H$). Note that H is a normal subgroup of $N(H)$. Construct a canonical isomorphism*

$$N(H)/H \simeq \operatorname{Aut}_{K\text{-Alg}}(L').$$

Week 8, Problem 10. *Let $L' \subset L$ be an arbitrary subextension. Consider the following subextensions:*

(a) *The extension obtained by adjoining to L' all the roots of the minimal polynomials of all elements of L' over K;*

(b) *The extension obtained by adjoining to L' all the roots of the minimal polynomials of a set of generators of L' over K;*

(c) *The extension generated by all $g(L')$, $g \in G$;*

(d) *The intersection of all Galois subextensions containing L';*

(e) *The subextension corresponding to the subgroup*

$$\bigcap_{g \in G} g \operatorname{Stab}(L') g^{-1} \subset G.$$

Show that all of the above subextensions coincide. The resulting subextension is called the Galois closure *of L'.*

16.5. **The inverse problem.**

16.5.1. Let now L be an arbitrary field, and let G be a finite group acting on L by automorphisms such that the map

$$G \to \operatorname{Aut}(L)$$

is injective. Set $K := L^G$. We will prove:

Theorem 16.5.2. *The extension $L \supset L^G$ is finite and Galois, and the map*

$$G \to \operatorname{Gal}(L/L^G) = \operatorname{Aut}_{K\text{-Alg}}(L)$$

is an isomorphism.

Proof. Choose, for each $g \in G$, a $y_g \in L$ such that $g(y_g) \neq y_g$ (one exists by the injectivity hypothesis on the map $G \to \operatorname{Aut}(L)$). Let $L' := K(\{h \cdot y_g \,|\, g, h \in G\})$, the field extension generated over K by the G-orbits of the y_g's. Since the set of generators is sent into itself by G, G leaves L' invariant. This gives a map $G \to \operatorname{Aut}_{K\text{-Alg}}(L')$. In fact this is injective, since L' contains each y_g.

Next the claim is that L'/K is Galois. Let $x \in L'$. Let $H := \operatorname{Stab}(x) \subseteq G$. Let

$$p(t) := \prod_{g \in G/H} (t - gx) \in L'[t].$$

Notice that p is G-invariant. Hence its coefficients actually lie in $(L')^G \subseteq L^G = K$ (actually equality holds). Since $p(x) = 0$ by construction, x is then algebraic over K. In fact it is also separable, since p has distinct roots and already splits completely over L'. Hence L'/K is a finite separable extension (since it is generated by finitely many algebraic and separable elements).

In fact we have done one better: the minimal polynomial of x over K certainly divides $p(t)$, so that in fact the minimal polynomial of x over K must split into linear factors in L' as well. Hence L'/K is normal, whence Galois.

But, regarding G as a subgroup of $\mathrm{Gal}(L'/K) = \mathrm{Aut}_{K\text{-Alg}}(L')$, since $(L')^G \subseteq K$ the fundamental theorem of Galois theory tells us that $G \to \mathrm{Gal}(L'/K)$ was in fact an isomorphism.

The final claim is that $L' = L$. Suppose otherwise. Let $x \in L - L'$. Consider $L'' := L'(gx, g \in G)$. In exactly the same way, by considering the polynomial

$$\prod_{g \in G/\,\mathrm{Stab}(x)} (t - gx) \in K[t]$$

we see that L''/K is also Galois. The map $G \to \mathrm{Gal}(L''/K)$ is still injective (because each $y_g \in L''$ too). But $L'' \subset L$ implies $(L'')^G \subset K$, so again by the fundamental theorem of Galois theory we see that $G \simeq \mathrm{Gal}(L''/K)$. In particular $\deg(L'/K) = |G| = \deg(L''/K)$, so that $L' = L''$. Contradiction.

□

17. Tuesday, April 2

17.1. **Problems in general Galois theory.** Let $K \subset L$ be a Galois extension, and let

$$K \subset L_i \subset L,\ i = 1, 2$$

be subextensions.

Week 9, Problem 1.

(a) *Show that* $\mathrm{Stab}(L_1 \cap L_2)$ *is the subgroup of* $\mathrm{Gal}(L/K)$*, generated by* $\mathrm{Stab}(L_1)$ *and* $\mathrm{Stab}(L_2)$*.*

(b) *Consider the field* $L_1L_2 \subset L$ *generated by* L_1 *and* L_2*. Show that it is the fixed field of* $\mathrm{Stab}(L_1) \cap \mathrm{Stab}(L_2)$*.*

Week 9, Problem 2. *Let* $K \subset L_1, L_2 \subset L' \subset L$ *be as above with* L_1 *normal. Show that*

$$\deg(L_1L_2/K)\deg(L_1 \cap L_2/K) = \deg(L_1/K)\deg(L_2/K).$$

17.2. **Finite fields.**

17.2.1. We start with the field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Note that if K is a finite extension of $\mathbb{F}_p$ of degree n, then

$$|K| = |\mathbb{F}_p|^n = p^n.$$

(Do you see why?)

We will prove:

Theorem 17.2.2. *For every* n *there exists a unique, up to isomorphism, extension of* $\mathbb{F}_p$ *of degree* n*.*

Proof. Consider an algebraic closure $\overline{\mathbb{F}}_p$. Consider the set

$$\mathbb{F}_{p^n} := \{x \in \overline{\mathbb{F}}_p,\ x^{p^n} = x.\}$$

The formula

$$(x_1 + x_2)^p = x_1^p + x_2^p$$

(valid in characteristic p — this because the binomial coefficients $\binom{p}{k} \equiv 0 \bmod p$ for $0 < k < p$) implies that $\mathbb{F}_{p^n}$ is indeed a field.

We claim that $|\mathbb{F}_{p^n}| = p^n$. Indeed, $\mathbb{F}_{p^n}$ is the set of roots in $\overline{\mathbb{F}}_p$ of the polynomial $f(t) = t^{p^n} - t$. This polynomial has no multiple roots (since $f'(t) = -1$, which is coprime to $f(t)$), so the number of roots equals the degree, p^n.

This implies that $\deg(\mathbb{F}_{p^n}/\mathbb{F}_p) = n$. This shows the existence of an extension of degree n.

Let now K be some other extension of degree n. We need to construct an isomorphism $K \simeq \mathbb{F}_{p^n}$. Choose an embedding $\phi : K \hookrightarrow \overline{\mathbb{F}}_p$. It suffices to show that $\mathrm{Im}(\phi) \subset \mathbb{F}_{p^n}$ by comparing sizes. The latter is equivalent to showing that

$$\phi(x)^{p^n} = \phi(x), \quad x \in K.$$

That is, we must show $x^{p^n} = x$ for all $x \in K$. For $x = 0$ this is evident. For $x \neq 0$, observe that $K^\times$ is a multiplicative group of size $|K^\times| = |K| - 1 = p^n - 1$. Hence by Lagrange's theorem we see that $x^{p^n - 1} = 1$ in K. Multiplying through by x gives the claim.

□

As a byproduct of the above proof, we obtain:

Corollary 17.2.3. *Every finite extension of $\mathbb{F}_p$ is Galois.*

Proof. Let K be such an extension of degree n. The fact that $K/\mathbb{F}_p$ is normal follows from the fact that its image under any embedding into $\overline{\mathbb{F}}_p$ is $\mathbb{F}_{p^n}$. The fact that $K/\mathbb{F}_p$ is separable follows from the fact that each of its elements satisfies the polynomial $f(t) = t^{p^n} - t$, which has no multiple roots. □

Hence we have shown that *any*(!) extension of finite fields is Galois. (After all, the point is that we are adjoining a $(p^n - 1)$-st root of unity to get from $\mathbb{F}_p$ to $\mathbb{F}_{p^n}$.)

17.2.4. *The multiplicative group of a finite field.* We claim:

Proposition 17.2.5. *Let $\mathbb{F}_q$ be a finite field with q elements. Then the group $\mathbb{F}_q^\times$ is cyclic.*

(That is, it is noncanonically isomorphic to $\mathbb{Z}/(q-1)\mathbb{Z}$.)

Proof. We have $|\mathbb{F}_q^\times| = q - 1$. Hence, by the classification of finite abelian groups (namely, the fact that every finite abelian group is a product of cyclic groups), it suffices to show that there is no $m < q - 1$ such that $x^m = 1$ for all $x \in \mathbb{F}_q$ (do you see why?). This follows from the fact that the polynomial $t^m - 1$ can only have at most m roots in $\mathbb{F}_q$ (since $\mathbb{F}_q$ is a field). □

17.2.6. Let's now calculate $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. There is an evident element in this Galois group, namely the Frobenius automorphism $x \mapsto x^p$. The point will be that this is essentially the *only* automorphism of a finite field — namely, its powers will generate the Galois groups of all the Galois extensions of $\mathbb{F}_p$, and similarly for the $\mathbb{F}_q$.

Now to the calculation. First, we define a homomorphism

$$\mathbb{Z}/n\mathbb{Z} \to \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p). \tag{17.1}$$

Namely, we let the generator $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ act on $\mathbb{F}_{p^n}$ by the Frobenius automorphism, defined by

$$\mathrm{Frob}_p(x) = x^p.$$

By the construction of $\mathbb{F}_{p^n}$, we have $\mathrm{Frob}_p^n = \mathrm{Id}$ (this because $x^{p^n} = x$ for all $x \in \mathbb{F}_{p^n}$), so we do indeed obtain a homomorphism as in (17.1).

Theorem 17.2.7. *The homomorphism* (17.1) *is an isomorphism.*

Proof. The two groups have the same order, so it is enough to show that (17.1) is injective. If it were not injective, this would mean that for some $m < n$, we would have $\mathrm{Frob}_p^m = \mathrm{Id}$ — i.e.,

$$x^{p^m} = x, \quad \forall\, x \in \mathbb{F}_{p^n},$$

which would mean that all elements of $\mathbb{F}_{p^n}$ are roots of the polynomial $t^{p^m} - t$. Contradiction. □

17.2.8. It is easy to see (by iterating Frobenius) that if $m|n$, then

$$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}.$$

(Equivalently, if $x^{p^m} = x$ and $md = n$, then, raising everything to the p^m-th power, $x^{p^{2m}} = x^{p^m} = x$. Repeating $(d-1)$ more times tells us that $x^{p^n} = x$.)

Vice versa, if $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$, then (since the latter is a vector space over the former)

$$|\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^d$$

for $d := \deg(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$, and so

$$p^n = (p^m)^d = p^{md}$$

— i.e., $m|n$. Hence $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ if and only if $m|n$.

In fact these isomorphisms are compatible:

Proposition 17.2.9. *Let $m|n$. Write $n = dm$. Then the subgroup*

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) \subset \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$$

identifies with

$$\mathbb{Z}/d\mathbb{Z} \subset \mathbb{Z}/n\mathbb{Z}, \quad \overline{1} \mapsto \overline{m}.$$

(That is, $\mathbb{Z}/d\mathbb{Z}$ is the (cyclic) kernel of the reduction mod m map $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.)

Proof. This follows from the commutative diagram

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \xrightarrow{(17.1)} & \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \\ \downarrow & & \downarrow \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow{(17.1)} & \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p). \end{array}$$

□

Note that under the above identification (with $q := p^m$)

$$\mathbb{Z}/d\mathbb{Z} \simeq \mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q),$$

the generator $\overline{1} \in \mathbb{Z}/d \cdot \mathbb{Z}$ acts on $\mathbb{F}_{q^d}$ as Frob_q, where

$$\mathrm{Frob}_q(x) := x^q.$$

17.3. **Cyclotomic extensions.** Let K be a field and n an integer coprime to $\mathrm{char}(K)$. (That is, $n \neq 0$ in K.)

17.3.1. Let $\mu_n(\overline{K})$ denote the group of n-th roots of unity inside $\overline{K}$.

Proposition 17.3.2. *The group $\mu_n(\overline{K})$ is (non-canonically) isomorphic to $\mathbb{Z}/n\mathbb{Z}$.*

Proof. Repeats that of Proposition 17.2.5. (Namely, choose a primitive n-th root of unity.) □

17.3.3. Let $K(\mu_n)$ denote the extension of K obtained by adjoining the elements $\mu_n(\overline{K})$. This is called the *n-th cyclotomic extension of K*. It is quite a beautiful field, especially over $\mathbb{Q}$.

By Proposition 17.3.2,

$$\deg(K(\mu_n)/K) \leq n.$$

The extension $K(\mu_n)$ is normal (we have adjoined all roots of the polynomial $p(t) = t^n - 1$) and separable (this polynomial has no multiple roots since $p'(t) = nt^{n-1}$ is coprime to $p(t)$). Thus, $K(\mu_n)$ is Galois over K.

17.3.4. Let

$$\mu_n(\overline{K})^{\mathrm{prim}} \subset \mu_n(\overline{K})$$

be the subset of *primitive* n-th roots of unity, i.e., those $\zeta \in \mu_n(\overline{K})$ such that $\zeta^m \neq 1$ for any $0 < m < n$.

In other words, primitive n-roots of unity are exactly those elements of $\mu_n(\overline{K})$ that generate it as an abelian group.

Lemma 17.3.5. *Let ζ be an element of $\mu_n(\overline{K})^{\mathrm{prim}}$. Then $K(\mu_n) = K(\zeta)$.*

Proof. Clear, since all other elements of $\mu_n(\overline{K})$ are powers of ζ. □

Hence these so-called *cyclotomic extensions* are obtained by adjoining a single (primitive) n-th root of unity. So from now on we will choose a primitive n-th root of unity ζ_n and write $K(\zeta_n)$ instead of $K(\mu_n)$.

Now to the properties of this Galois extension. First of all, what can we say about its Galois group?

17.3.6. We will define a group homomorphism

$$\mathrm{Gal}(K(\zeta_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^\times, \tag{17.2}$$

where $(\mathbb{Z}/n\mathbb{Z})^\times$ is the group of invertible elements in the *ring* $\mathbb{Z}/n\mathbb{Z}$.

First, we claim:

Lemma 17.3.7. *Multiplication defines an isomorphism of groups*

$$(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}_{\mathrm{Ab}}(\mathbb{Z}/n\mathbb{Z}).$$

Proof. For any commutative ring R, multiplication by elements of $R^\times$ defines a group isomorphism

$$R^\times \to \mathrm{Aut}_{R\text{-mod}}(R).$$

Hence $(\mathbb{Z}/n\mathbb{Z})^\times$ maps isomorphically to $\mathrm{Aut}_{(\mathbb{Z}/n\mathbb{Z})\text{-mod}}(\mathbb{Z}/n\mathbb{Z})$. However

$$\mathrm{Aut}_{(\mathbb{Z}/n\mathbb{Z})\text{-mod}}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathrm{Aut}_{\mathbb{Z}\text{-mod}}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathrm{Aut}_{\mathrm{Ab}}(\mathbb{Z}/n\mathbb{Z}),$$

where the first isomorphism takes place since the action of $\mathbb{Z}$ factors through that of $\mathbb{Z}/n\mathbb{Z}$, and the second isomorphism expresses the fact that abelian groups are the same as $\mathbb{Z}$-modules. □

(Another way to say this is: look at where $\overline{1}$ goes.)

Corollary 17.3.8. *There is a* canonical *isomorphism*

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathrm{Aut}_{\mathrm{Ab}}(\mu_n(\overline{K})).$$

Proof. We define the map of *monoids*

$$\mathbb{Z} \to \mathrm{End}_{\mathrm{Ab}}(\mu_n(\overline{K}))$$

by sending $m \in \mathbb{Z}$ (here $\mathbb{Z}$ is viewed as a monoid under the operation of *multiplication*) to the endomorphism of $\mu_n(\overline{K})$ given by

$$\zeta_n \mapsto \zeta_n^m.$$

This map factors through a map of monoids

$$\mathbb{Z}/n\mathbb{Z} \to \mathrm{End}_{\mathrm{Ab}}(\mu_n(\overline{K}))$$

since $\zeta_n^n = 1$.

Hence, it induces a map of the corresponding groups of invertible elements

$$(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}_{\mathrm{Ab}}(\mu_n(\overline{K})).$$

The fact that this map is an isomorphism follows from Proposition 17.3.2 and Lemma 17.3.7.

□

Another way to say this is that an automorphism of the abelian group $\mu_n(\overline{K})$ takes our chosen primitive n-th root of unity ζ_n to ζ_n^m for some m. But then the fact that this preserves products entirely determines the map once we know m. Moreover, since ζ_n was primitive so must ζ_n^m be, whence m and n must be coprime. Finally, none of this depends on the choice of primitive n-th root of unity ζ_n (do you see why?).

17.3.9. Hence, to define the map (17.2), we need to make $\mathrm{Gal}(K(\zeta_n)/K)$ act by automorphisms of the abelian group $\mu_n(\overline{K})$. The latter is given by acting on $\mu_n(\overline{K}) \subset K(\zeta_n)$ (a field automorphism determines an automorphism of the set of roots of any polynomial — in this case we are taking the polynomial to be $t^n - 1$).

Explicitly, an element $\sigma \in \mathrm{Gal}(K(\zeta_n)/K)$ gets sent to the unique element $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that

$$\sigma(\zeta_n) = \zeta_n^m.$$

17.3.10. We now claim:

Proposition 17.3.11. *The map* (17.2) *is injective.*

Proof. This follows from the fact that an automorphism of $K(\zeta_n)$ over K fixes the elements of $\mu_n(\overline{K})$ if and only if it fixes the generator ζ_n, if and only if it fixes all elements of $K(\zeta_n)$. □

Corollary 17.3.12. *The Galois group* $\mathrm{Gal}(K(\zeta_n)/K)$ *is abelian.*

17.4. **Cyclotomic extensions of $\mathbb{Q}$.** We now take $K = \mathbb{Q}$.

17.4.1. Let n be a positive integer. The *cyclotomic polynomial* $\Phi_n(t)$ is defined inductively by the equality

$$\prod_{m|n} \Phi_m(t) = t^n - 1.$$

(Here $\Phi_1(t) := t-1$, and note that this product includes Φ_n!) By Galois invariance a priori we know that $\Phi_n(t) \in \mathbb{Q}[t]$. In fact it lies in $\mathbb{Z}[t]$ thanks to Gauss's lemma and induction (this because it appears in a factorization of the monic integral polynomial $t^n - 1$ as a product of two monic polynomials with rational coefficients, hence integral coefficients, and, as we will see in a second, for n prime $\Phi_n(t)$ has integer coefficients.).

This is probably the most significant polynomial appearing in algebraic number theory. The cyclotomic extensions "cut out" by it arise quite naturally when studying reciprocity laws (e.g., the quadratic, cubic, and quartic reciprocity laws are most naturally stated in terms of $\mathbb{Q}$, $\mathbb{Q}(\zeta_3)$ (commonly denoted $\mathbb{Q}(\omega)$), and $\mathbb{Q}(i)$). They also arose quite naturally in elementary attempts at resolving Fermat's Last Theorem in the late 1800s. Of course they also played an absolutely fundamental role in the not-so-elementary resolution of the problem some hundred years later.

For example, let p be a prime. Then the only divisors of p are 1 and p, so that

$$\Phi_p(t) = \frac{t^p - 1}{t - 1} = t^{p-1} + \cdots + t + 1.$$

Let's now actually verify the assertion made about the roots of $\Phi_n(t)$.

Lemma 17.4.2. *Over* $\overline{\mathbb{Q}}$,

$$\Phi_n(t) = \prod_{\zeta \in \mu_n(\overline{\mathbb{Q}})^{\mathrm{prim}}} (t - \zeta).$$

Proof. The roots of $t^n - 1$ are precisely the primitive d-th roots of unity for $d|n$. Thus the claim follows by induction. □

Corollary 17.4.3. $\deg(\Phi_n(t)) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

(This because we know the number of primitive n-th roots of unity!)

Write $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$. This is known as *Euler's totient function.* (For example, $\phi(1) = 1, \phi(p) = p - 1$, and $\phi(p^n) = p^{n-1}(p-1)$.) It is also the number of positive integers $1 \leq k \leq n$ that are coprime to k (i.e., for which $\gcd(k, n) = 1$). By the Chinese remainder theorem it is *multiplicative*: if a and b are coprime positive integers, $\varphi(ab) = \varphi(a)\varphi(b)$.

Corollary 17.4.4. $\sum_{d|n} \varphi(d) = n$.

Now to a fundamental theorem.

Theorem 17.4.5 (Gauss)**.** *The polynomial* $\Phi_n(t) \in \mathbb{Z}[t]$ *is irreducible.*

Corollary 17.4.6. $\Phi_n(t)$ *is the minimal polynomial over* $\mathbb{Q}$ *for all the primitive* n*-th roots of unity.*

Proof. Evident from Theorem 17.4.5. □

Corollary 17.4.7. *The map* (17.2)

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

is an isomorphism.

Proof. By Theorem 17.4.5, $\mathbb{Q}(\zeta_n) = \mathbb{Q}[t]/(\Phi_n(t))$. Hence the sizes of the left- and right-hand sides agree. But the map was already injective. □

17.4.8. *Irreducibility of the Cyclotomic Polynomial (Optional).* There are an incredible number of proofs of the irreducibility of the cyclotomic polynomials over $\mathbb{Q}$. (Go look online to see many, many beautiful proofs from the olden days.) Here is one.

Proof of Theorem 17.4.5. Suppose $f(t)$ is a nonconstant monic polynomial in $\mathbb{Q}[t]$ dividing $\Phi_n(t)$. Then its roots (in $\overline{\mathbb{Q}}$) are all primitive n-th roots of unity. If we can show that, for p a prime not dividing n, and ζ a root of f (so $f(\zeta) = 0$ and it is a primitive n-th root of unity),

$$f(\zeta^p) = 0,$$

then the claim is that $f(t) = \Phi_n(t)$ and we are done. Namely, if ζ_n is any root of f over $\overline{\mathbb{Q}}$, then ζ_n^m is a root of f for any m that is a product of prime powers coprime to n (Proof: iterate the previous claim to get prime powers or products of prime powers.). That is to say, *all* primitive n-th roots of unity are roots of f.

So let's show the claim. Let p a prime not dividing n. Write

$$\Phi_n(t) =: f(t)g(t).$$

By Gauss's lemma $f, g \in \mathbb{Z}[t]$. Suppose for the sake of contradiction that ζ is a root of f but ζ^p is a root of g. Consider the ring

$$\mathbb{Z}[\zeta] \subset \mathbb{Q}(\zeta).^4$$

Let (p) be the ideal generated by $p \in \mathbb{Z} \subset \mathbb{Z}[\zeta]$ in this ring. Let

$$(p) \subset \mathfrak{p} \subset \mathbb{Z}[\zeta]$$

be any maximal ideal containing it. Then $\mathbb{Z}[\zeta]/\mathfrak{p} =: \mathbb{F}_\mathfrak{p}$ is a field, and we have a canonical quotient map

$$\mathbb{Z}[\zeta]/(p) \twoheadrightarrow \mathbb{F}_\mathfrak{p}.$$

Let $\bar{f} \in \mathbb{F}_p[t]$ be the reduction of $f \in \mathbb{Z}[t]$ modulo p (i.e., reduce all the coefficients of f modulo p to get $\bar{f}$). Now remember the equality of polynomials

$$\bar{f}(t^p) = \bar{f}(t)^p \pmod{p}.$$

Since $(p) \subset \mathfrak{p}$, this tells us that, as polynomials now thought of inside $\mathbb{F}_\mathfrak{p}[t]$,

$$\bar{f}(t^p) \equiv \bar{f}(t)^p \pmod{\mathfrak{p}}.$$

But then, since the right-hand side is zero (in $\mathbb{F}_\mathfrak{p}$) at $t = \bar{\zeta} \in \mathbb{F}_\mathfrak{p}$, so is the left-hand side. So

$$\bar{f}(\bar{\zeta}^p) = \bar{g}(\bar{\zeta}^p) = 0 \in \mathbb{F}_\mathfrak{p}.$$

That is to say,

$$(t - \bar{\zeta}^p) \mid \bar{f}(t), \bar{g}(t).$$

[4]This is called the "ring of integers" of this field — the analogue of $\mathbb{Z} \subset \mathbb{Q}$.

But then $(t-\bar{\zeta}^p)^2 \,|\, \bar{f}(t)\bar{g}(t) = \overline{\Phi}_n(t)$ and $\overline{\Phi}_n(t) \,|\, t^n - \bar{1}$, so

$$(t-\bar{\zeta}^p)^2 \,|\, t^n - \bar{1}.$$

But, since $t^n - \bar{1}$ is coprime to its derivative $\bar{n}t^{n-1}$ in $\mathbb{F}_{\mathfrak{p}}$ (since $\bar{n} \neq 0$ in $\mathbb{F}_{\mathfrak{p}}$ (equivalently, $p \nmid n$)), this is a contradiction. □

17.4.9. Here is another proof in the particular case when $n = p^m$ is a power of a prime p.

Proof. Note that for $n = p^m$, we have

$$\Phi_n(t) = \frac{t^{p^m}-1}{t^{p^{m-1}}-1} = t^{p^{m-1}(p-1)} + t^{p^{m-1}(p-2)} + \ldots + t^{p^{m-1}} + 1, \tag{17.3}$$

and note that this is a polynomial with coefficients in $\mathbb{Z}$.

To prove that $\Phi_n(t)$ is irreducible, it suffices to show that the polynomial $\Phi_n(t+1)$ is irreducible. We will use the following (elementary) assertion, known as the Eisenstein criterion:

Lemma 17.4.10. *Let p be a prime. Let*

$$f(t) = a_n t^n + \cdots + a_0 \in \mathbb{Z}[t]$$

such that

- *a_n is coprime to p (e.g., it is 1);*
- *For $0 < i < n$, $p \,|\, a_i$;*
- *$p^2 \nmid a_0$.*

Then $f(t)$ is irreducible.

Proof. Take a factorization and reduce it modulo p. The point is that $f(t) \equiv a_n t^n \pmod{p}$, and if $gh = f$ is a nontrivial factorization, then g, h are congruent (up to nonzero constants) to powers of t modulo p. In particular p divides their constant terms. Hence $p^2 \,|\, g(0)h(0) = f(0)$. Contradiction. □

Let us check that the conditions of Eisenstein's criterion hold for $\Phi_n(t+1)$. First, from (17.3), it is easy to see that $\Phi_n(t+1)$ is monic, and that its constant term is p. Hence it remains to show that p divides all the rest of the coefficients. But $(t+1)^{p^m} - 1 \equiv t^{p^m} \pmod{p}$. Hence, since $\Phi_n(t+1)\left((t+1)^{p^{m-1}} - 1\right) = \left((t+1)^{p^m} - 1\right)$,

$$\Phi_n(t) \equiv t^{p^{m-1}(p-1)} \pmod{p}.$$

□

Week 9, Problem 3. *Let $K \subset L$ be a Galois extension, and let $x \in L$ be an element such that the subextension $K(x)$ is normal. Show that in this case* $\deg(K(x)/K)$ *equals the number of elements in the orbit of x under the action of* $\mathrm{Gal}(L/K)$.

Week 9, Problem 4. *Let ζ_7 be a seventh root of unity in $\overline{\mathbb{Q}}$. Consider the elements $a = \zeta_7 + \zeta_7^5$; $b = \zeta_7 + \zeta_7^4$; $c = \zeta_7^3 + \zeta_7^5 + \zeta_7^6$. Calculate the degrees of the corresponding extensions $\mathbb{Q}(a)/\mathbb{Q}$, $\mathbb{Q}(b)/\mathbb{Q}$; $\mathbb{Q}(c)/\mathbb{Q}$.*

17.5. **Kummer extensions.** Let K be a field, and let n be an integer co-prime to $\mathrm{char}(K)$. In this subsection we will assume that K contains $\mu_n(\overline{K})$.

17.5.1. Let $a \in K^\times$ be an element. Consider the extension $K(a^{\frac{1}{n}})$ obatined by adjoining to K *an* n-th root of the element a inside an algebraic closure. (Such a thing is called a *Kummer extension* of K.) We will prove:

Proposition 17.5.2. *The extension $K(a^{\frac{1}{n}}) \supset K$ is Galois, and its Galois group admits an injection into $\mu_n(K) = \mu_n(\overline{K})$.*

Proof. Let B denote the set

$$\{b \in L \,|\, b^n = a.\}$$

Note that the group $\mu_n(K)$ acts on B by multiplication. This action is simply-transitive. (That is, for each $b, b' \in B$ there is a *unique* $\zeta \in \mu_n(K)$ such that $b = \zeta b'$. Namely, divide b by b'.)

Hence, since $K(a^{\frac{1}{n}})$ contains one element of B, it contains all of them. I.e., $K(a^{\frac{1}{n}})$ contains all the roots of the polynomial $t^n - a$. Hence, $K(a^{\frac{1}{n}})$ is normal over K.

The extension $K(a^{\frac{1}{n}}) \supset K$ is separable, because its generator satisfies the polynomial $t^n - a$, which is coprime to its derivative. Thus $K(a^{\frac{1}{n}})$ is Galois over K.

The action of $\mathrm{Gal}(K(a^{\frac{1}{n}})/K)$ on $K(a^{\frac{1}{n}})$ defines an action of $\mathrm{Gal}(K(a^{\frac{1}{n}})/K)$ on the set B. This action commutes with the above action of $\mu_n(K)$ on B. We have the following general lemma:

Lemma 17.5.3. *Let G be a group acting on a set X. Let A be an abelian group that acts on X simply-transitively. Assume that the actions of G and A on X commute with each other. Then the action of G factors through a homomorphism $G \to A$.*

(After all, X is isomorphic to A upon choosing a point $x \in X$, and the commutativity hypothesis tells us that this does not affect the map $G \to A$ thus produced.)

Applying the lemma, we obtain that the action of $\mathrm{Gal}(K(a^{\frac{1}{n}})/K)$ on B factors through a homomorphism

$$\chi : \mathrm{Gal}(K(a^{\frac{1}{n}})/K) \to \mu_n(K).$$

I.e.,

$$\sigma(b) = \chi(\sigma)b, \quad b \in B.$$

Finally, we claim that the homomorphism χ is injective. Indeed, if an element $\sigma \in \mathrm{Gal}(K(a^{\frac{1}{n}})/K)$ is such that $\chi(\sigma) = 1$, we obtain that $\sigma(b) = b$ for a generator b of $K(a^{\frac{1}{n}})$ over K, and hence $\sigma = 1$.

□

Here is an entirely equivalent, but perhaps more elementary way of phrasing the above argument. The reason we have phrased it in this way is that it is this argument that generalizes to producing explicit extensions with abelian Galois groups over certain fields of tremendous number-theoretic interest (like $\mathbb{Q}$). (This is called "explicit class field theory".)

Second proof. The minimal polynomial of $a^{\frac{1}{n}}$ divides $t^n - a$. The roots of this polynomial are $\zeta a^{\frac{1}{n}}$ for $\zeta \in \mu_n(K)$. Hence $t^n - a$, and thus the minimal polynomial of $a^{\frac{1}{n}}$ splits into linear factors. Moreover, these are all distinct since $a \neq 0$. Hence the minimal polynomial of $a^{\frac{1}{n}}$ is separable, too. Thus, since the extension is generated by $a^{\frac{1}{n}}$, it is Galois.

Finally, let

$$\mathrm{Gal}(K(a^{\frac{1}{n}})/K) \to \mu_n(K)$$

via

$$\sigma \mapsto \frac{\sigma(a^{\frac{1}{n}})}{a^{\frac{1}{n}}}.$$

Namely, since $\sigma\left(a^{\frac{1}{n}}\right)$ is also a root of $t^n - a$, it is of the form $\zeta a^{\frac{1}{n}}$ for some $\zeta \in \mu_n(K)$. The map sends σ to this ζ.

This is injective because if σ fixes $a^{\frac{1}{n}}$ then it fixes the whole field.

□

Corollary 17.5.4. $\deg(K(a^{\frac{1}{n}})/K) \mid n$.

Proof. This follows from the fact that $|\mathrm{Gal}(K(a^{\frac{1}{n}})/K)|$ divides $|\mu_n(K)|$. □

17.5.5. We now claim:

Theorem 17.5.6. *Suppose that a is not an m-th power in K for any $m \mid n$ ($m \neq 1$, of course). Then polynomial $t^n - a$ is irreducible in $K[t]$ and the map*

$$\chi : \mathrm{Gal}(K(a^{\frac{1}{n}})/K) \to \mu_n(K)$$

is an isomorphism.

Proof. Of course the second statement follows from the first because, assuming the first, the left- and right-hand sides have cardinality n (since then $K(a^{\frac{1}{n}}) = K[t]/(t^n - a)$), and we've already seen that the map is injective.

Let $f(t) \in K[t]$ be the minimal polynomial of $b := a^{\frac{1}{n}} \in \overline{K}$ (our fixed n-th root of a) over K. Since the Galois group of $K(a^{\frac{1}{n}})/K$ embeds into $\mu_n(K)$, $\deg(f) \mid n$.

Now $f(t) = \prod_{\zeta \in B}(t - \zeta b)$ in $\overline{K}[t]$ for some $B \subset \mu_n(K)$. The constant term is, up to a product of n-th roots of unity and a sign (all of which are contained in K), $b^{\deg(f)}$. Hence $b^{\deg(f)} \in K$. But then $\left(b^{\deg(f)}\right)^{\frac{n}{\deg(f)}} = a$, exhibiting a as a $\frac{n}{\deg(f)}$-th power in K. Hence $\deg(f) = n$, whence $f(t) = t^n - a$, as desired.

□

Week 9, Problem 5. *Let ζ_7 be a primitive seventh root of unity in $\overline{\mathbb{Q}}$. Show that the extension $\mathbb{Q}(\zeta_7, 2^{\frac{1}{7}})/\mathbb{Q}$ is Galois, and compute its Galois group.*

18. Thursday, April 4

18.1. **The canonical extension with Galois group S_n.** The moral point of this section will be that a "random Galois extension" (i.e., the Galois closure of a field $K[t]/(f(t))$ for some polynomial $f \in K[t]$, say of degree n, chosen "randomly") will have Galois group S_n. We won't actually say anything about this precisely, but it is a useful thing to keep in mind for the future. This section will also answer the question of which finite groups arise as Galois groups of *some* extension L/K (any L, any K). There is considerable interest at present of resolving the question of which finite groups arise as Galois groups of an extension with $K = \mathbb{Q}$.

18.1.1. Let k be a field, and consider the field

$$L = k(X_1, \ldots, X_n)$$

of rational functions in the x_i (i.e., quotients of polynomials in the n variables X_i).

Consider the polynomial

$$f(t) := \prod_{i=1}^{n}(t - X_i) \in L[t].$$

Write

$$f(t) =: t^n - a_1 t^{n-1} + \cdots + (-1)^i a_i t^{n-i} + \cdots + (-1)^n a_n.$$

The element $a_i \in k(X_1, \ldots, X_n)$ for $i = 1, \ldots, n$ is called the i-th elementary symmetric polynomial (also denoted $e_i = e_i(X_1, \ldots, X_n)$) in $X_1, \ldots, X_n$. In general

$$a_i = \sum_{J \in \binom{[n]}{i}} \prod_{j \in J} X_j,$$

the sum taken over subsets $J \subset [n] := \{1, \ldots, n\}$ of size i (hence the notation "$[n]$ choose i" for the set of such subsets).

For example,

$$a_1 = X_1 + \cdots + X_n \text{ and } a_n = \prod_{i=1}^{n} X_i.$$

We let K be the subfield of L generated over k by the elements $a_1, \ldots, a_n$. By construction $f(t)$ is an element of $K[t]$. Note that the elements $\{X_1, \ldots, X_n\}$ are exactly the roots of $f(t)$ in L.

18.1.2. We have:

Proposition 18.1.3. *The extension L/K is finite.*

Proof. The extension $L \supset K$ is generated by the elements $X_1, \ldots, X_n$, each of which is a root of $f(t)$. Hence all these elements are algebraic over K. Since there are finitely many of them, we obtain that L/K is finite. □

Remark 18.1.4. Using the notion of *transcendence degree* one can show that K is isomorphic to the field of rational functions over k on the variables $a_1, \ldots, a_n$ (the proof will be posted as a mini-project).

From this point of view $f(t) \in K[t]$ is the *universal polynomial of degree n over k with freely adjoined coefficients $a_1, \ldots, a_n$*:

$$f(t) = t^n + \cdots + (-1)^i a_i t^i + \cdots + (-1)^n a_n.$$

18.1.5. We now claim:

Lemma 18.1.6. *The extension $L \supset K$ is a finite Galois extension.*

Proof. Same as that of Proposition 18.1.3. (This because the X_i are distinct, so f is separable, and f also splits in L.) □

Finally, we have:

Theorem 18.1.7. *The Galois group of L/K identifies with S_n.*

Proof. We make S_n act on L by permuting the generators $X_1, \ldots, X_n$. This action leaves the polynomial $f(t)$ invariant. Hence its coefficients $a_1, \ldots, a_n$ are S_n-invariant. Hence $K \subset L^{S_n}$. This defines a map

$$S_n \to \mathrm{Gal}(L/K).$$

We define the inverse map $\mathrm{Gal}(L/K) \to S_n$ as follows.

Since $f(t) \in K[t]$, the action of $\mathrm{Gal}(L/K)$ maps the set of roots of $f(t)$ to itself. I.e., we obtain an action of $\mathrm{Gal}(L/K)$ on the set $\{X_1, \ldots, X_n\}$, which is the same as a map $\mathrm{Gal}(L/K) \to S_n$.

Now, the two maps are mutually inverse "on the nose."

□

Corollary 18.1.8. *Any element of $k(X_1, \ldots, X_n)$, invariant under the action of S_n, can be expressed as a ratio of polynomials in the elements $a_1, \ldots, a_n$.*

Proof. This follows from the fact that $L^{S_n} = K$. □

Remark 18.1.9. One can show if $p \in k[X_1, \ldots, X_n]$ (rather than $k(X_1, \ldots, X_n)$) is invariant under the action of S_n (called a *symmetric polynomial*), then p is actually a *polynomial* in the elements $a_1, \ldots, a_n$ (the so-called *elementary symmetric polynomials*). This is the *fundamental theorem of symmetric polynomials.*

In particular the sum of k-th powers of the X_i are polynomials in the a_i. These polynomials were determined by Newton and give "Newton's identities".

Corollary 18.1.10. *Any finite group can be realized as a Galois group.*

Proof. Let G be a finite group. We can always realize it as a subgroup of S_n for some n ($G \to S_{|G|}$ via acting on itself by e.g. left-multiplication). The sought-for extension is $L \supset L^G$. □

18.1.11. Consider the subfield $L' := L^{S_{n-k}}$, where $S_{n-k} \subset S_n$ is the stablizer of the elements

$$\{X_1, \ldots, X_k\} \subset \{X_1, \ldots, X_n\}.$$

It is clear that

$$K(X_1, \ldots, X_k) \subset L'.$$

Week 9, Problem 6. *Show that the inclusion $K(X_1, \ldots, X_k) \subset L'$ is an equality.* Hint: mimic the proof of Theorem 18.1.7.

18.1.12. We will now study the subextension $K(X_1)$. According to Problem 6,

$$K(X_1) = L^{S_{n-1}}.$$

Corollary 18.1.13. *The polynomial $f(t) \in K[t]$ is irreducible.*

Proof. We have

$$\deg(K(X_1)/K) = \deg(L^{S_{n-1}}/K) = |S_n/S_{n-1}| = n.$$

Since X_1 satisfies the polynomial $f(t)$, and f is of degree n, f must then be its minimal polynomial. □

Remark 18.1.14. Using Remark 18.1.4, we obtain that $K(X_1)$ is the field isomorphic to

$$K[t]/(f(t)),$$

i.e., the field obtained by adjoining to $K = k(a_1, \ldots, a_n)$ the root of the "universal" polynomial

$$t^n + \cdots + (-1)^i a_i t^i + \cdots + (-1)^n a_n.$$

18.1.15. Finally, we claim:

Proposition 18.1.16. *The Galois closure of $K[t]/(f(t))$ is all of L.*

Proof. This follows from [Week 8, Problem 10]. □

18.2. **Another proof of the fundamental theorem of Galois theory.** In this subsection we will discuss a slightly different proof of Theorem 16.3.6. Let L/K be a Galois extension with Galois group G.

18.2.1. Recall the maps

$$\{\text{subextensions of } K \subset L\} \to \{\text{subgroups of } G\}, \quad L' \rightsquigarrow \mathrm{Stab}(L')$$

and

$$\{\text{subgroups of } G\} \to \{\text{subextensions of } K \subset L\}, \quad H \rightsquigarrow L^H.$$

We will give a direct proof of:

Theorem 18.2.2. *The composition*

$$\{\textit{subextensions of } K \subset L\} \to \{\textit{subgroups of } G\}, \to \{\textit{subextensions of } K \subset L\}$$

is the identity map.

Proof. We need to show that, for a subextension $K \subset L' \subset L$, the inclusion

$$L' \subset L^{\mathrm{Stab}(L')}$$

is an equality.

Note that L/L' is a Galois extension. Hence the desired result follows from:

Proposition 18.2.3. *Let L/K be Galois and $x \in L - K$. Then there exists an element $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(x) \neq x$.*

(This is of course obvious once we know the fundamental theorem of Galois theory! But that would be circular.)

□

Proof of Proposition 18.2.3. Let $p(t) \in K[t]$ be the minimal polynomial of x. Since L/K is normal and separable, there exists $x \neq y \in L$ with $p(y) = 0$. Let ϕ denote the map $K(x) \to L$ that sends $x \mapsto y$. We need to show this map can be extended to a map of extensions $L \to L$. However, this results from the following:

Lemma 18.2.4. *Let $K \subset L' \subset L$ be finite extensions, where L/K is normal. Then any map of extensions $\phi : L' \to L$ can be extended to a map $L \to L$.*

(The lemma follows by combining Proposition 14.2.6 and the definition of normality in Proposition 14.3.2(4). Alternatively, it immediately reduces to the case of $L = L'(x) \simeq L'[t]/(g(t))$, where g is the minimal polynomial of $x \in L$ over L'. Let f be the minimal polynomial of $x \in L$ over K. Then $\phi(g)|\phi(f) = f$ in $L'[t]$. But by normality, since $f(x) = 0$, f splits into linear factors in $L[t]$. Hence the same goes for $\phi(g)$. Let y be any root of $\phi(g)$ in L. Take $x \mapsto y$.)

□

Week 9, Problem 7. *Let $K \subset L$ be a Galois extension, and let L_1, L_2 be two subextensions. Let $G \supset H_1, H_2$ denote the Galois groups of L/K, L/L_1 and L/L_2, respectively. Show that the set of maps of extenions $L_1 \to L_2$ is canonically isomorphic to the quotient of the set*

$$\{g \in G \,|\, gH_1g^{-1} \supset H_2\}$$

by the equivalence relation

$$g' \sim g'' \Leftrightarrow \exists\, h_1 \in H_1 \text{ such that } g' \cdot h_1 = g''.$$

18.2.5. From Theorem 18.2.2 we obtain:

Corollary 18.2.6. *The map*

$$\{\text{subextensions of } K \subset L\} \to \{\text{subgroups of } G\}$$

is injective.

Corollary 18.2.7. *A finite Galois extension has finitely many subextensions.*

Proof. This follows from the fact that its (finite) Galois group has only finitely many subgroups. □

Corollary 18.2.8. *A finite separable extension has finitely many subextensions.*

Proof. A separable extension embeds into a Galois closure (e.g., if an extension $L = K[x_1, \ldots, x_n]/K$ is separable, then adjoining all the roots of the minimal polynomials of the x_i over K to L, we get a Galois extension). □

18.3. **The other direction.** We will now give a direct proof of:

Theorem 18.3.1. *The composition*

$$\{\text{subgroups of } G\} \to \{\text{subextensions of } K \subset L\} \to \{\text{subgroups of } G\}$$

is the identity map.

Proof. We need to show that for a subgroup $H \subset G$, the inclusion

$$H \subset \mathrm{Stab}(L^H)$$

is an equality.

Since L is Galois over $L^H = L^{\mathrm{Stab}(L^H)}$, the desired result follows from:

Proposition 18.3.2. *Let L/K be a Galois extension with Galois group G. Let $H \subset G$ be a subgroup such that $L^H = K$. Then $H = G$.*

□

We will give a proof of Proposition 18.3.2 using the Primitive Element Theorem.

18.3.3. The Primitive Element Theorem reads:

Theorem 18.3.4. *Let $K \subset L$ be a finite separable extension. Then there exists an element $x \in L$ such that $L = K(x)$.*

We will give two proofs of Theorem 18.3.4: one in Sect. 18.4, and the other as a mini-project.

Let us show how Theorem 18.3.4 implies Proposition 18.3.2:

Proof of Proposition 18.3.2. Let $x \in L$ be such that $K(x) = L$. Consider the polynomial

$$g(t) := \prod_{h \in H} (t - h(x)) \in L[t].$$

By construction, $g(t)$ is H-invariant, so it belongs to $K[t]$. Let $f(t)$ be the minimal polynomial of x over K. Since $g(x) = 0$, $f | g$ in $K[t]$. But:

$$|G| = \deg(L/K) = \deg(f(t)) \leq \deg(g(t)) = |H| \leq |G|,$$

whence the inclusion $H \subset G$ must have been an equality.

□

18.4. **Proof of the Primitive Element Theorem.** We will prove the following assertion:

Theorem 18.4.1. *Let $K \subset L$ be a finite extension. Then the following are equivalent:*

(a) *L is uni-generated over K, i.e., there exists $x \in L$ such that $L = M(x)$.*

(b) *There are only finitely many subextensions $K \subset L' \subset L$.*

This theorem implies the Primitive Element Theorem in view of Corollary 18.2.8.

18.4.2. *Proof of (a) ⇒ (b).* Let $x \in L$ be such that $K(x) = L$. Let $p(t) \in K[t]$ be the minimal polynomial of x over K. We claim that there exists an injection of sets

$$\{\text{subextensions of L}\} \hookrightarrow \{\text{factors of } p(t) \text{ as a polynomial with coefficients in } L\}.$$

(Of course there are only finitely many of the latter.)

Indeed, let L_1 be a subextension. Let $p_1(t)$ be the minimal polynomial of x over L_1. Then, since $p(x) = 0$, $p_1(t) \,|\, p(t)$ in $L_1[t]$. We claim that $p_1(t)$ determines L_1 uniquely. Namely, let

$$\{a_0, a_1, \ldots, a_n\} \subset L_1$$

be the coefficients of $p_1(t)$. Let $L_1' := K(a_0, a_1, \ldots, a_n) \subset L_1$. The claim is that this inclusion is an equality. (So our injection takes L_1 to $p_1(t)$.)

Indeed, the polynomial $p_1(t)$ belongs to $L_1'[t]$. It is irreducible over L_1, and hence also over L_1'. Hence,

$$\deg(L_1'(x)/L_1') = \deg(p_1(t)).$$

Since $p_1(t)$ was the minimal polynomial of x over L_1, we also have that

$$\deg(L_1(x)/L_1) = \deg(p_1(t)).$$

But $L = K(x) \subset L_1'(x) \subset L_1(x) \subset L$, so that $L_1(x) = L_1'(x) = L$, whence

$$\deg(L/L_1') = \deg(L/L_1).$$

This gives the claim (since $L_1' \subset L_1$ and $\deg(L_1/K) = \frac{\deg(L/K)}{\deg(L/L_1)} = \frac{\deg(L/K)}{\deg(L/L_1')} = \deg(L_1'/K)$).

□

18.4.3. *Proof of (b) ⇒ (a): the case when K is infinite.* It is enough to show that, given $x, y \in L$ there exists a third element $z \in L$ such that

$$K(x, y) \subset K(z).$$

(Proof: $L = K(x_1, \ldots, x_n)$ for some x_i. Now apply the claim inductively to reduce the number of generators n down to 1.)

Consider the elements $x + \lambda y \in L$ for $\lambda \in K$. Since K was assumed infinite, and there are only finitely many subextensions, there exist $\lambda \neq \mu$ such that

$$K(x + \lambda y) = K(x + \mu y) = K(z)$$

for $z := x + \lambda y$. But $x = \frac{\mu(x+\lambda y) - \lambda(x+\mu y)}{\mu - \lambda} \in K(z)$ and $y = \frac{(x+\lambda y) - (x+\mu y)}{\lambda - \mu} \in K(z)$ (the point is that $\lambda \neq \mu$, so we can divide).

□

18.4.4. *Proof of (b) ⇒ (a): the case when K is finite.* We have $K = \mathbb{F}_q$ and $L = \mathbb{F}_{q^d}$ for some d. The group $\mathbb{F}_{q^d}^\times$ is cyclic, as we've seen. Let $x \in \mathbb{F}_{q^d}^\times$ be a generator, so that $x^d \neq 1$ for any $0 < d < q^d - 1$. But of course $\mathbb{F}_{q^d} = \mathbb{F}_q(x)$: we don't even need sums of powers, since every nonzero element is just a power of x!

□

18.4.5. Theorem 18.4.1 also allows us to produce examples of finite extensions (automatically inseparable) that are not uni-generated.

Namely, let $K = k(X_1, X_2)$, rational functions in X_1, X_2, where $\mathrm{char}(k) = p$, and k is *not* a finite field (for example, take $k = \mathbb{F}_p(T)$, rational functions in T). Let

$$L := K(X_1^{\frac{1}{p}}, X_2^{\frac{1}{p}}).$$

We claim that L/K is not uni-generated. Namely, we will show that it fails condition (b) of Theorem 18.4.1.

First, it is easy to see that the field L is isomorphic to the field of rational functions (over k) in the variables $X_1^{\frac{1}{p}}$ and $X_2^{\frac{1}{p}}$ — i.e.,

$$L \simeq k(X_1^{\frac{1}{p}}, X_2^{\frac{1}{p}}).$$

Now consider the elements $X_1^{\frac{1}{p}} + \lambda X_2^{\frac{1}{p}}$, and the corresponding fields

$$K \subset K(X_1^{\frac{1}{p}} + \lambda X_2^{\frac{1}{p}}) \subset L.$$

We claim that these extensions are all distinct. Indeed, as in the proof of the implication (b) ⇒ (a), if two such extensions coincide, we obtain that there exists an element $\lambda \in k$ such that

$$X_2^{\frac{1}{p}} \in K(X_1^{\frac{1}{p}} + \lambda X_2^{\frac{1}{p}}) =: L'.$$

Let $Y := X_1 + \lambda^p X_2$. Via a change of variables, we see that

$$L \simeq k(Y^{\frac{1}{p}}, X_2^{\frac{1}{p}}).$$

The subextension L' then identifies with

$$k(Y^{\frac{1}{p}}, X_2) \subset k(Y^{\frac{1}{p}}, X_2^{\frac{1}{p}}).$$

From here it is manifest that $X_2^{\frac{1}{p}} \notin L'$.

Hence since k was assumed infinite, this is a separable extension with infinitely many subextensions, whence it is not uni-generated.

19. Tuesday, April 9

What follows is a totally ubiquitous finiteness condition in algebra. (Recall that, to get reasonable theorems, we had to assume vector spaces were finite dimensional, or modules were finitely generated. In this case the definition we are about to give turns out to be equivalent to requiring that all submodules of a finitely generated module are also finitely generated, which isn't a property that follows for free (but life would certainly be horrible without it!).)

19.1. **Noetherianness.**

19.1.1. Let R be a ring. We shall say that R is (left-)Noetherian if every (left) ideal in R is finitely generated.

Lemma 19.1.2. *The following conditions on a ring R are equivalent:*

(a) *R is Noetherian.*

(b) *There does not exist an infinite increasing chain of ideals*

$$I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq \cdots$$

with strict *containments.*

(That is, every increasing chain of ideals stabilizes — i.e., there is an n sufficiently large for which $I_n = I_{n+k}$ for all $k > 0$.)

Proof. For (a) $\Rightarrow$ (b), for a chain as above, set

$$I = \bigcup_n I_n.$$

It is easy to see that I is an ideal. Let $f_1, \ldots, f_n$ be generators for I. For each $i = 1, \ldots, n$ there exists an index k such that $f_i \in I_k$. Hence, there exists an index k such that all

$$f_1, \ldots, f_n \in I_k.$$

But then $I_k = I$. Contradiction.

For (b) $\Rightarrow$ (a), let I be an ideal that is not finitely generated. We construct elements $f_0, f_1, \ldots, f_n, \ldots \in I$ inductively. Set $f_0 = 0$, set $I_n = (f_0, f_1, \ldots, f_n)$, and let $f_{n+1} \in I$ be any element that does not belong to I_n (one exists by assumption). Then

$$I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq \cdots$$

is a chain of ideals with strict containments.

□

19.1.3. *Examples.* Any PID (principal ideal domain) is Noetherian (since every ideal is even *uni*-generated). So $\mathbb{Z}$ is Noetherian.

Any field is Noetherian (there are only two ideals: (0) and (1) (the whole thing)).

Shortly, we will see that the rings $\mathbb{Z}[t_1, \ldots, t_n]$ and $k[t_1, \ldots, t_n]$ are Noetherian (this will follow from Hilbert's basis theorem, i.e., Theorem 19.1.10). Hence, any quotient thereof is also Noetherian, because of:

Lemma 19.1.4. *A quotient of a Noetherian ring is Noetherian.*

Proof. Take the preimage of a given ideal, find generators, and then project them back down. □

19.1.5. *A non-example.* Consider the ring

$$R = k[t_1, t_2, \ldots],$$

the polynomial ring on infinitely many variables. It is *not* Noetherian. Here's a chain with proper containments:

$$(t_1) \subsetneq (t_1, t_2) \subsetneq (t_1, t_2, t_3) \subsetneq \cdots .$$

19.1.6. Here is a very important result about Noetherian rings, alluded to earlier (in fact, one might say this is the purpose of considering Noetherianness in the first place):

Theorem 19.1.7. *For a ring R the following are equivalent:*

(a) *R is Noetherian.*

(b) *A submodule of a finitely generated module is finitely generated.*

Proof. The implication (b) $\Rightarrow$ (a) is tautological: take the (evidently finitely generated!) module R over itself. An R-submodule is just an ideal. Let us now prove (a) $\Rightarrow$ (b). Let M be a finitely generated module, and $M' \subset M$ a submodule.

Finite generation of M means that there exists a surjection $R^n \twoheadrightarrow M$. This reduces the assertion to the case when $M = R^n$ (take the preimage of M'). We will argue by induction on n. The base case is the assumption of (a). Assume that the statement is true for $n-1$. Consider the short exact sequence

$$0 \to R^{n-1} \to R^n \to R \to 0,$$

and the resulting short exact sequence

$$0 \to (R^{n-1} \cap M') \to M' \to M'/(R^{n-1} \cap M') \to 0.$$

By the induction hypothesis, $R^{n-1} \cap M'$ is finitely generated. The module $M'/(R^{n-1} \cap M')$ maps injectively to $R^n/R^{n-1} \simeq R$ (an isomorphism of R-modules). Hence it too is finitely generated. Thus the assertion follows from the following (obvious) lemma:

Lemma 19.1.8. *If, in the short exact sequence*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

M_1 and M_3 are finitely generated, then so is M_2.

(Prove it!)

□

19.1.9. Now to Hilbert's basis theorem:

Theorem 19.1.10. *If R is Noetherian, then so is $R[t]$.*

Before you read the proof, give it a try. The proof is short, but it contains a really quite beautiful idea. When Gordan, who was the world expert in invariant theory at the time (and had been trying to prove a result of this shape for years via explicit calculation) read this proof, he exclaimed,

"This is not Mathematics, it is Theology!"[5]

Phrased in this language, the idea has already been had — namely, the proof will proceed by showing existence, rather than by actually constructing a finite set of generators for an ideal.

Proof. Let $I \subset R[t]$ be an ideal. The claim is that it is finitely generated. Let $J \subset R$ be the subset formed by the highest coefficients of elements of I:

$$J = \{a \,|\, \exists n, a_i : at^n + a_{n-1}t^{n-1} + \cdots \in I\}.$$

It is easy to see that J is an ideal. Let $r_1, \ldots, r_n \in R$ be generators for J. Let $f_1, \ldots, f_n$ be elements of R whose highest coefficients are $r_1, \ldots, r_n$, respectively. Let $d_i := \deg(f_i)$. Set $d := \max(d_1, \ldots, d_n)$.

Consider the R-submodule $R[t]^{\leq d}$ of polynomials of degree $\leq d$. Set

$$M := I \cap R[t]^{\leq d}.$$

Then M is an R-module, which is an R-submodule of $R[t]^{\leq d} \simeq R^{d+1}$. By Theorem 19.1.7, M too is finitely generated! Let $g_1, \ldots, g_m$ be generators.

We claim that the elements

$$f_1, \ldots, f_n, g_1, \ldots, g_m$$

generate I. The point is that we can keep dividing by the f_i to get down to something of degree at most d, and then get what's left with the g_j. Namely, let

$$p =: a_n t^n + \cdots \in I.$$

If $n > d$, write

$$a_n =: \sum c_i r_i \in J.$$

Then

$$p - \sum c_i t^{n-d_i} f_i$$

has t^n term equal to zero by construction, hence is degree at most $n-1$. Thus by induction $p - \sum c_i t^{n-d_i} f_i$ is of degree at most d. It is also in the ideal. Hence it is equal to $\sum \tilde{c}_i g_i$ for some $\tilde{c}_i \in R$. But then

$$p = \sum c_i t^{n-d_i} f_i + \sum \tilde{c}_j g_j,$$

as desired.

□

19.2. **Prime ideals.** From now on, all rings will be assumed commutative.

[5]Soon after: "I have convinced myself that even Theology has its advantages." (See page 121 of Doxiadis and Mazur, *Circles Disturbed.*)

19.2.1. An ideal $\mathfrak{p} \subset A$ is called *prime* if

$$a, b \notin \mathfrak{p} \Rightarrow ab \notin \mathfrak{p}.$$

The idea here is that this is the proper generalization of notion of primeness in $\mathbb{Z}$. (Recall Euclid's lemma that a prime divides a product if and only if it divides one of the factors. *This* is the essential step in proving unique factorization in $\mathbb{Z}$.)

Lemma 19.2.2. *An ideal $\mathfrak{p}$ is prime if and only if the quotient ring $A/\mathfrak{p}$ is a domain (i.e. it has no zero divisors — elements $a, b \neq 0$ such that $ab = 0$).*

The point is that a ring is a domain if and only if the ideal (0) is prime. (Do you see why?)

19.2.3. For the remainder of this subsection, A will be a *domain*.

Let us recall the following definition:

Definition 19.2.4. *An nonzero element $f \in A$ is called* prime *(or* irreducible*) if it is* not *invertible, and*

$$f = f_1 f_2 \Rightarrow f | f_1 \text{ or } f | f_2.$$

(That is, there are no nontrivial factorizations of f — of course $f = (u^{-1})(uf)$ for u a unit is a factorization of f. Namely,)

Lemma 19.2.5. *Let $f \in A$ be prime. Then if $f = f_1 f_2$ and $f | f_1$, then f_2 is invertible.*

Proof. Write $f_1 =: fg$. Then $f = f \cdot g \cdot f_2$. Hence

$$f \cdot (1 - g f_2) = 0,$$

and, since A is a domain, $g \cdot f_2 = 1$, as desired. □

Proposition 19.2.6. *Let A be Noetherian. Then any non-zero and non-invertible element in A can be written as a product of prime elements.*

If we were to start trying to prove unique factorization for all rings, the natural thing would be to first produce factorizations for every element into irreducible elements. This says that for *Noetherian* rings, the natural process will terminate. However, the real strength in unique factorization is the *uniqueness*, and this isn't at all true for a general ring (even a Noetherian ring!).

Proof. Suppose not, and let f_1 be an element contradicting the claim. Then certainly f_1 isn't prime. Write

$$f_1 = f_2 \cdot g_2 \text{ with } f_1 \nmid f_2, \ f_1 \nmid g_2.$$

In particular, the containments $(f_1) \subset (f_2)$ and $(f_1) \subset (g_2)$ are strict. By assumption, f_2 and g_2 aren't both prime. Without loss of generality f_2 isn't prime. Repeat:

$$f_2 = f_3 \cdot g_3 \text{ with } f_2 \nmid f_3, \ f_2 \nmid g_3,$$

etc. We obtain a chain

$$(f_1) \subsetneq (f_2) \subsetneq \cdots$$

with strict contaiments. □

19.2.7. *Prime ideals and prime elements.* We observe:

Lemma 19.2.8. *If the ideal (f) is prime, then the element f is prime.*

Proof. If $f = f_1 \cdot f_2$, then $f_1 \cdot f_2 \in (f)$. Hence at least one of these elements belongs to (f), as desired. □

The converse does *not* necessarily hold! (This is why people study prime ideals all the time, and prime elements almost never.)

19.2.9. Recall:

Definition 19.2.10. *A ring A is called a UFD if:*

- *Every non-invertible element $f \in A$ can be written as a product of prime elements;*
- *For two such decompositions*

$$\prod_{i=1}^{m} f_i = \prod_{i=1}^{n} g_i,$$

we have $m = n$, and for every i there exists a j such that $f_i = g_j \cdot u_j$, where u_j is a unit.

(Do you see why this is the usual unique factorization in $\mathbb{Z}$?)

For example, any PID is a UFD — see Lemma 19.3.6. Hence $\mathbb{Z}, k[t]$, etc. are all UFDs. In fact, Gauss's lemma tells us that if R is a UFD, then $R[t]$ is a UFD, too. (Do you see why?)

19.2.11. Now let's show the converse of Lemma 19.2.8 for unique factorization domains.

Lemma 19.2.12. *Let A be a UFD. Then f prime implies (f) prime.*

Proof. Let f be prime, and let $f_1 \cdot f_2 \in (f)$, i.e., $f_1 \cdot f_2 = f \cdot g$ for some $g \in A$. Choosing prime decompositions of f_1, f_2 and g, we obtain that f divides at least one factor of a prime decomposition of f_1 or f_2, whence it divides one of them, as desired. □

Week 10, Problem 1. *Let $A := \{p(t) \,|\, p'(0) = 0\} \subset k[t]$. Show that A is* not *a UFD.*

Finally, we claim:

Proposition 19.2.13. *Assume that every element in A can be written as a product of prime elements*[6]*. Then A is a UFD if and only if f prime implies (f) prime.*

Proof. We've already seen the forward direction.

For the reverse, let $\prod_{i=1}^{m} f_i = \prod_{i=1}^{n} g_i$ be two factorizations of the same element into irreducibles. Consider f_1. Since f_1 is prime, (f_1) is prime, and also

$$\prod_{i=1}^{n} g_i \in (f_1).$$

[6]According to Proposition 19.2.6, this is the case whenever A is Noetherian.

Hence there exists an index j (without loss of generality, $j = 1$) so that $g_j = g_1 \in (f_1)$. That is, $f_1 \,|\, g_1$. Since g_1 is prime, we have $g_1 = f_1 \cdot u_1$, where u_1 is a unit. Divide out by f_1 and continue by induction.

□

19.3. **Maximal ideals.**

19.3.1. An ideal $\mathfrak{m} \subset A$ is called maximal if $\mathfrak{m} \neq A$ and it is maximal with respect to this property (under inclusion) That is, $\mathfrak{m} \subsetneq I \subseteq A$ implies $I = A$.

Prime ideals correspond to quotients that are domains, and maximal ideals correspond to quotients that are:

Lemma 19.3.2. *An ideal $\mathfrak{m} \subset A$ is maximal if and only if $A/\mathfrak{m}$ is a field.*

Proof. An ideal $I \subset A$ is maximal if and only if $\{0\}$ is maximal in A/I. The latter property is equivalent to being a field (that is, a ring is a field if and only if its only ideals are (0) and (1)). □

Corollary 19.3.3. *A maximal ideal is prime.*

Proof. A field is a domain. □

19.3.4. *Existence of maximal ideals.*

Proposition 19.3.5. *For a ring A and a proper ideal $I \subsetneq A$, there exists a maximal ideal $\mathfrak{m}$ containing I.*

Week 10, Problem 2. *Deduce Proposition 19.3.5 from Zorn's lemma. Now assume that A is Noetherian and prove the claim without using Zorn's lemma.*

Lemma 19.3.6. *Any PID is a UFD. In fact, any nonzero prime ideal in a PID is maximal.*

Proof. Let A be a PID. It is Noetherian, so it is enough to show that "f prime" implies "(f) prime."

Let f be prime. Let $f \in \mathfrak{m}$ be any maximal ideal containing f. Since A is a PID, $\mathfrak{m} = (g)$ for some g. Hence $f = g \cdot h$ for some h. By assumption g is not invertible (or else $\mathfrak{m} = A$). Hence, since f is prime, h is invertible. Hence $(f) = (g) = \mathfrak{m}$. Hence (f) is maximal, and hence prime. □

19.4. **The Nullstellensatz.**

19.4.1. Let k be a field. Let $A := k[t_1, \ldots, t_n]$. Any element $\underline{c} = (c_1, \ldots, c_n) \in k^n$ defines a homomorphism of k-algebras

$$\mathrm{ev}_{\underline{c}} : A \to k, \quad f(t) \mapsto f(\underline{c})$$

via evaluation.

This homomorphism is surjective. (Do you see why?) Hence

$$\mathfrak{m}_{\underline{c}} := \ker(\phi_{\underline{c}})$$

is a maximal ideal.

Week 10, Problem 3. *Show that the ideals $\mathfrak{m}_{\underline{c}}$ are pairwise distinct.*

19.4.2. Here is a truly amazing (and kind of shocking, if you think about it) theorem:

Theorem 19.4.3 (Hilbert's Nullstellensatz)**.** *Let k be algebraically closed. Then any maximal ideal in $k[t_1, \dots, t_n]$ is of the form $\mathfrak{m}_{\underline{c}}$ for some $\underline{c} \in k^n$.*

Note that for $n = 1$, all this theorem says is that any maximal ideal in $k[t]$ is generated by $(t - c)$ for some $c \in k$. But we know that already. However, already for $n > 1$ the assertion of the theorem is extremely nontrivial. It is the starting point of the *entirety* of algebraic geometry.

Week 10, Problem 4. *Let A be a finitely generated k-algebra (i.e., an algebra that can be realized as a quotient of $k[t_1, \dots, t_n]$ for some n). Deduce the following from the Nullstellensatz: any maximal ideal in A is of the form* $\ker(\phi)$*, where ϕ is a homomorphism of k-algebras $A \to k$.*

Week 10, Problem 5. *Show that the assertion of the Nullstellensatz is equivalent to the following: if k is algebraically closed, then for any field extension $k \subset K$, if K is finitely generated* as a k-algebra*, then $k = K$.*

Note the difference between the following notions for a field extension $k \subset K$:

- being finitely generated as a k-module (i.e., being a finite field extension);
- being finitely generated as a k-algebra (which is what Problem 5 talks about);
- being finitely generated as a field extension (i.e., $K = k(t_1, \dots, t_n)$ for some $t_i \in K$).

20. Thursday, April 11

All rings will again be assumed commutative.

20.1. **Localization of rings.**

20.1.1. Let $S \subset A$ be a subset that contains 1 and does not contain 0. We shall say that S is a *multiplicative* subset of A if it is closed under multiplication: $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$.

For example, if A is a domain, we can take $S := A - \{0\}$.

More generally, for any prime ideal $\mathfrak{p} \subset A$, we can take $S := A - \mathfrak{p}$.

Also, if $f \in A$ is a non-nilpotent element, we can take $S := \{1, f, f^2, \dots\}$.

These cover the essential examples.

20.1.2. Given a multiplicative set S, we construct a new ring A_S as follows. Its elements are symbols

$$\frac{a}{s}, \quad a \in A, s \in S$$

modulo the following equivalence relation:

$$\frac{a}{s} = \frac{b}{t} \text{ if there exists } u \in S \text{ such that } u(a \cdot t - s \cdot b) = 0. \tag{20.1}$$

— i.e., if and only if $a \cdot t \cdot u = b \cdot s \cdot u$.

(The naive equivalence relation would be to just cross multiply and set that equal to zero, but in fact that doesn't work if A is not a domain.)

Multiplication on A_S is defined by the rule

$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} := \frac{a_1 \cdot a_1}{s_1 \cdot s_2},$$

and addition is defined by

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 \cdot s_2 + a_2 \cdot s_1}{s_1 s_2}.$$

(Just like you'd expect from the notation!)

Check for yourself that the above formulas are well-defined (i.e., that they respect the equivalence relation (20.1)), and give rise to a ring structure on A_S.

20.1.3. For example, if A is a domain and $S := A - \{0\}$, the ring A_S is (by definition) the fraction field of A. (Do you see why it is a field? What is it in the case of $A = \mathbb{Z}$?)

For a prime ideal $\mathfrak{p}$ and $S := A - \mathfrak{p}$, the corresponding ring A_S is denoted $A_{\mathfrak{p}}$ (rather than $A_{A-\mathfrak{p}}$).

For a non-nilpotent element $f \in A$ and $S := \{1, f, f^2, \ldots\}$, the corresponding localization is denoted A_f.

Week 10, Problem 6. *Let $f \in A$ be a non-nilpotent element. Construct an isomorphism $A_f \simeq A[t]/(ft - 1)$.*

Note that Problem 6 implies that if A is finitely generated *as an algebra* over a field k, then so is A_f.

20.1.4. *The universal property of localization.* Note that we have a canonical homomorphism

$$\phi_{univ} : A \to A_S, \quad a \mapsto \frac{a}{1}.$$

For $s \in S$, the element $\phi_{univ}(s) \in A_S$ is *invertible*. Its inverse is given by $\frac{1}{s} \in A_S$.

We now claim that A_S is "universal" with respect to this property — namely:

Proposition 20.1.5. *Let $\phi : A \to B$ be a ring homomorphism such that $\phi(s) \in B$ is invertible for every $s \in S$. Then there exists a unique ring homomorphism $\widetilde{\phi} : A_S \to B$ such that $\phi = \widetilde{\phi} \circ \phi_{univ}$.*

Proof. Define $\widetilde{\phi}$ by the formula

$$\widetilde{\phi}\left(\frac{a}{s}\right) := \phi(a) \cdot (\phi(s))^{-1}.$$

Check that this does the job (and is even well-defined in the first place!). □

20.2. **Ideals in a localization.**

20.2.1. We construct a map

$$\{\text{Ideals in } A\} \to \{\text{Ideals in } A_S\}$$

by sending an ideal $I \subset A$ to the subset $I_S \subset A_S$ that consists of elements that can be written as

$$\frac{a}{s}, \quad a \in I.$$

It is easy to see that I_S is indeed an ideal in A_S.

Proposition 20.2.2.

(a) *The ideal I_S is proper if and only if $S \cap I = \emptyset$.*

(b) *If $I = \mathfrak{p}$ is prime and $\mathfrak{p} \cap S = \emptyset$, then $\mathfrak{p}_S \subset A_S$ is prime.*

Proof. For point (a), $I_S = A_S$ if and only if $\frac{1}{1} \in I_S$, which means that there exist $a \in I$ and $s \in S$ such that

$$\frac{1}{1} = \frac{a}{s},$$

i.e., there exists $t \in S$ such that $ts = ta$. But $ts = ta$ would be both in S and I. Conversely, if $a \in I \cap S$, then $a \cdot 1 = 1 \cdot a$ implies that $\frac{1}{1} = \frac{a}{a} \in I_S$.

For point (b), suppose

$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} \in \mathfrak{p}_S.$$

This means that there exist $a \in \mathfrak{p}$ and $s, t \in S$ such that

$$t \cdot s \cdot a_1 \cdot a_2 = t \cdot s_1 \cdot s_2 \cdot a.$$

The RHS belongs to $\mathfrak{p}$, hence so does the LHS. But $\mathfrak{p}$ is prime, and $s, t \notin \mathfrak{p}$. Hence $a_1 \in \mathfrak{p}$ or $a_2 \in \mathfrak{p}$. In the former case $\frac{a_1}{s_1} \in \mathfrak{p}_S$, and in the latter case $\frac{a_2}{s_2} \in \mathfrak{p}_S$. □

Week 10, Problem 7. *Assume that $S \cap I = \emptyset$, and let π denote the projection map $A \to A/I$. Construct an isomorphism $A_S/I_S \simeq (A/I)_{\pi(S)}$.*

20.2.3. Note that if $\phi : A \to B$ is a homomorphism of rings we have a map

$$\{\text{Ideals in } A\} \to \{\text{Ideals in } B\}, \quad J \mapsto \phi^{-1}(J).$$

(Do you see why this is an ideal?)

Another way to describe this map is by noting that $\phi^{-1}(J)$ is the kernel of the map $A \to B \to B/J$. Hence $A/\phi^{-1}(J) \to B/J$ is an injection.

Lemma 20.2.4.

(a) *The above map sends prime ideals to prime ideals.*

(b) *If ϕ is surjective, the above map sends maximal ideals to maximal ideals.*

(Note that point (b) does not hold for general ϕ. For instance, (0) is maximal in $\mathbb{Q}$, but its preimage under $\mathbb{Z} \to \mathbb{Q}$ (namely, $(0) \subset \mathbb{Z}$) is no longer maximal.)

Proof. For point (a), as we saw above,

$$A/\phi^{-1}(J) \to B/J \tag{20.2}$$

is injective. Hence, if B/J has no zero divisors, nor does $A/\phi^{-1}(J)$.

For point (b), we note that if ϕ is surjective, then the map (20.2) is also surjective, and hence is an isomorphism. Hence, if one quotient is a field, then so is the other. □

Week 10, Problem 8.

(a) *Assume that A and B are algebras finitely generated over an algebraically closed field k, and that ϕ is a map of k-algebras. Show that the Nullstellensatz implies that in this case the preimage of a maximal ideal is maximal.*

(b, optional) *Assume the knowledge of the following theorem: for any map of finitely generated k-algebras, the preimage of a maximal ideal is maximal. Deduce the Nullstellensatz.*

20.2.5. Let us apply the construction of Sect. 20.2.3 to the map

$$\phi_{univ} : A \to A_S.$$

We obtain a map

$$\{\text{Ideals in } A_S\} \to \{\text{Ideals in } A\}, \quad J \mapsto \phi_{univ}^{-1}(J).$$

We shall denote this map by Sat_S ("Sat" stands for *saturation*). By Lemma 20.2.4, this map sends prime ideals to prime ideals.

Lemma 20.2.6. *If J is a proper ideal in A_S, then $\mathrm{Sat}_S(J) \cap S = \emptyset$.*

Proof. Do it yourself. □

We now claim:

Proposition 20.2.7.

(a) *For any $J \subset A_S$, we have $(\mathrm{Sat}_S(J))_S = J$.*

(b) *For any $I \subset A$ we have $I \subset \mathrm{Sat}_S(I_S)$.*

(c) *For a prime $\mathfrak{p} \subset A$ with $\mathfrak{p} \cap S = \emptyset$ we have $\mathfrak{p} = \mathrm{Sat}_S(\mathfrak{p}_S)$.*

Proof. For (a), for an element of $(\mathrm{Sat}_S(J))_S$, write it as $\frac{a}{s}$, where $a \in \mathrm{Sat}_S(J)$, i.e., $\frac{a}{1} \in J$. But then

$$\frac{a}{s} = \frac{a}{1} \cdot \frac{1}{s},$$

which belongs to J, since it is an ideal. Vice versa, for $\frac{a}{s} \in J$, we have $\frac{a}{1} \in J$ (by multiplying by s), and hence $a \in \mathrm{Sat}_S(J)$. Hence $\frac{a}{s} \in (\mathrm{Sat}_S(J))_S$.

Point (b) is evident. For point (c), it of course suffices to show the reverse inclusion. Assume that $a \in \mathrm{Sat}_S(\mathfrak{p}_S)$. Then $\frac{a}{1} = \frac{b}{s}$ with $b \in \mathfrak{p}$. But this means that there exists $t \in S$ such that

$$t \cdot s \cdot a = t \cdot b.$$

Hence, $t \cdot s \cdot a \in \mathfrak{p}$. However, $s, t \notin \mathfrak{p}$ and $\mathfrak{p}$ is prime, so $a \in \mathfrak{p}$.

□

Corollary 20.2.8. *There exists a canonical bijection*

$$\{\textit{Prime ideals in } A \textit{ that don't intersect } S\} \simeq \{\textit{Prime ideals in } A_S\}.$$

(The inverse bijections are given by saturation and "localization" (i.e., $I \mapsto I_S$).)

In particular,

Corollary 20.2.9. *For a prime ideal $\mathfrak{q}$ there is a canonical bijection*

$$\{\textit{Prime ideals in } A \textit{ contained in } \mathfrak{q}\} \simeq \{\textit{Prime ideals in } A_{\mathfrak{q}}\}.$$

(This because if $I \cap (A - \mathfrak{q}) = \emptyset$, then $I \subset \mathfrak{q}$.)

20.2.10. Here is a cool application of what we've done:

Theorem 20.2.11. *Let $f \in A$ be a non-nilpotent element. Then there exists a prime ideal $\mathfrak{p} \in A$ such that $f \notin \mathfrak{p}$.*

Proof. Consider the ring A_f. It is nonzero because f is non-nilpotent (namely, $1 \neq 0$). Let $\mathfrak{m}$ be a maximal ideal of A_f. Set $\mathfrak{p} = \mathrm{Sat}_f(\mathfrak{m})$. It does the job by Corollary 20.2.8.

□

Corollary 20.2.12. *The set of nilpotent elements in A equals the intersection of all primes of A.*

Proof. The fact that any element in the intersection of all primes is nilpotent follows from Theorem 20.2.11. The reverse direction is obvious:

$$f^n = 0 \in \mathfrak{p} \Rightarrow f \in \mathfrak{p}.$$

□

Week 10, Problem 9.

(a) *Deduce the following from the Nullstellensatz: let A be a finitely generated algebra over an algebraically closed field k. Then for any non-nilpotent element $f \in A$, there exists a k-algebra homomorphism $A \to k$ such that $\phi(f) \neq 0$. In particular, there exists a maximal ideal $\mathfrak{m} \subset A$ such that $f \notin \mathfrak{m}$.*

(b) *Deduce the following statement from (a). Let k be an algebraically closed field, and let $I \subset k[t_1, \ldots, t_n]$ be an ideal. Let $f \in k[t_1, \ldots, t_n]$ be an element with the following property: for every $\underline{c} \in k^n$ such that $g(\underline{c}) = 0$ for every $g \in I$, we also have $f(\underline{c}) = 0$. Then there exists an integer n such that $f^n \in I$.*

(c, optional) *Assume the statement from (b) and deduce from it the Nullstellensatz.*

(Point (b) is the classical version of the Nullstellensatz. The point is that if f vanishes on all the same points on which the elements of I all vanish, then *a power of* f must be in I. (If $f^2 \in I$, then certainly since $(f^2)(\underline{c}) = 0$ we have that $f(\underline{c}) = 0$.) But for instance the ideal $(t^2) \subset k[t]$ tells us that we can't do any better than this power business.)

20.3. **Local rings.**

20.3.1. A ring is called *local* if it has a unique maximal ideal.

Lemma 20.3.2. *Let A be a local ring and $\mathfrak{m} \subset A$ its unique maximal ideal. Then any element in $f \in A - \mathfrak{m}$ is invertible.*

Proof. If $f \notin \mathfrak{m}$, then the ideal (f) is not contained in $\mathfrak{m}$, and hence equals all of A by Proposition 19.3.5. In particular, $1 \in (f)$. □

In fact, we have a converse assertion:

Proposition 20.3.3. *Let A be a ring and $I \subset A$ an ideal such that every element in $A - I$ is invertible. Then A is local with maximal ideal I.*

Week 10, Problem 10. *Prove Proposition 20.3.3.*

Corollary 20.3.4. *The ring $k[[t_1, \dots, t_n]]$ of formal power series in the variables $t_1, \dots, t_n$ is local, with maximal ideal $(t_1, \dots, t_n)$.*

Proof. We let $\mathfrak{m} := (t_1, \dots, t_n)$ be the ideal of power series constant term 0. It is easy to see that any formal power series with the free term non-zero is invertible. Indeed, with no restriction of generality (by scaling), it is enough to show that for $f \in \mathfrak{m}$ the element $1 - f$ is invertible. However, the (infinite!) series

$$1 + f + f^2 + \cdots$$

makes sense (the smallest term in f^n has degree n, so each coefficient (of a product of powers of the t_i) involves only a finite sum), and thus provides an inverse to $1 - f$. □

20.3.5. Let A be a ring and $\mathfrak{p}$ a prime ideal of A.

Proposition 20.3.6. *The ring $A_{\mathfrak{p}}$ is local.*

Proof. Follows from Corollary 20.2.9. □

20.3.7. We can also say something about the algebras appearing as summands in Theorem 13.2.5:

Proposition 20.3.8. *Let A be an algebra and $I \subset A$ an ideal such that every element in I is nilpotent, and A/I is a field. Then A is local with maximal ideal I.*

Proof. The ideal I is maximal because the quotient is a field. We claim that I is also contained in any maximal ideal. This follows from the (easy) direction of Corollary 20.2.12. □

20.4. **Localization of modules.**

20.4.1. Let $S \subset A$ be a multiplicative set and M an A-module. We define the A-module M_S in basically the same way as A_S. It is defined to be the set of equivalence classes of expressions

$$\frac{m}{s}, \quad m \in M, s \in S$$

modulo the following equivalence relation

$$\frac{m_1}{s_1} = \frac{m_2}{s_2} \text{ if there exists } s \in S \text{ such that } s \cdot s_2 \cdot m_1 = s \cdot s_1 \cdot m_2.$$

(This is just $M \otimes_A A_S$, as we will see.)

Note that in addition to being an A-module, M_S is actually an A_S-module:

$$\frac{a}{s} \cdot \frac{m}{s'} := \frac{a \cdot m}{ss'}.$$

In fact, we have the following:

Lemma 20.4.2. *For an A-module M, the action of A on M extends to an action of A_S if and only if every element of S acts on M invertibly. Such an extension is unique.*

Proof. Do it yourself. □

20.4.3. *The universal property.* Consider the canonical map

$$T_{univ} : M \to M_S, \quad m \mapsto \frac{m}{1}.$$

We have:

Proposition 20.4.4. *Let N be an A-module on which the elements of S act invertibly. Then for any $T : M \to N$ there exists a unique $\widetilde{T} : M_S \to N$ such that $T = \widetilde{T} \circ T_{univ}$.*

Proof. Given T, we define

$$\widetilde{T}(\frac{m}{s}) := (s\cdot)^{-1} \cdot \phi(m),$$

where $(s\cdot)^{-1}$ is the operator inverse to that of the action of $s \in A$ on M. Check that this does the job. □

20.4.5. We now claim (as noted above):

Proposition 20.4.6. *There exists a canonical isomorphism of A_S-modules:*

$$M_S \simeq A_S \underset{A}{\otimes} M.$$

Proof. Define a map $M_S \to A_S \underset{A}{\otimes} M$ by

$$\frac{m}{s} \mapsto \frac{1}{s} \otimes m.$$

It is easy to see that this is a well-defined map of A_S-modules.

Define a map $A_S \underset{A}{\otimes} M$ by

$$\frac{a}{s} \otimes m \mapsto \frac{a \cdot m}{s}.$$

Again, it is easy to see that this is a well-defined map of A_S-modules.

Moreover, it is easy to check that the above two maps are mutually inverse.

□

(Alternatively, both obey the same universal property.)

20.4.7. Note that a map of A-modules $T : M \to N$ gives rise to a map

$$T_S : M_S \to N_S, \quad \frac{m}{s} \mapsto \frac{\phi(m)}{s}.$$

We now claim (— this is a property extremely special to localization, making it a tremendously useful tool in mathematics):

Proposition 20.4.8. *Let*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

be a short exact sequence of A-modules. Then

$$0 \to (M_1)_S \to (M_2)_S \to (M_3)_S \to 0$$

is also short exact.

Proof. The fact that $(M_2)_S \to (M_3)_S$ is surjective is evident.

Let us show that $(M_1)_S \to (M_2)_S$ is injective. Denote the initial map $M_1 \to M_2$ by T. Let $\frac{m_1}{s} \in (M_1)_S$ be an element such that $T_S(\frac{m_1}{s}) = 0$. This means that $\frac{T(m_1)}{s} = 0$. I.e., there exists $s' \in S$ such that $s' \cdot T(m_1) = 0$. I.e., $T(s' \cdot m_1) = 0$. However, T is injective, so $s' \cdot m_1 = 0$. But this implies that $\frac{m_1}{s} = 0$.

The fact that

$$\mathrm{Im}((M_1)_S \to (M_2)_S) = \ker((M_2)_S \to (M_3)_S)$$

is proved similarly. (Do it!)

□

21. Tuesday, April 16

21.1. **The prime spectrum.**

21.1.1. Let A be a commutative ring. We let $\mathrm{Spec}(A)$ be the set of prime ideals in A. (This is called the *spectrum* of A.) For an ideal $I \subset A$, let $V(I) \subset \mathrm{Spec}(A)$ be the set

$$\{\mathfrak{p} \in \mathrm{Spec}(A) \,|\, I \subset \mathfrak{p}\}.$$

The idea here is that, given an operator T on a finite-dimensional vector space over an algebraically closed field k, one can form $k[T] := k[t]/(p(t))$, where p is the minimal polynomial of T. Then the spectrum of this ring is precisely the spectrum of T as an operator (i.e., the primes are of the form $(t - \lambda)$ for λ an eigenvalue of T on V).

Of course the canonical example is $\mathbb{C}^n$, realized as the maximal ideals in the spectrum $\mathrm{Spec}\,(\mathbb{C}[t_1, \ldots, t_n])$ — this is the Nullstellensatz. So this spectrum construction recovers (in a nice way) the idea of studying only polynomial functions on $\mathbb{C}^n$ (by taking the maximal ideals containing a given ideal). Algebraic geometry concerns itself with the vanishing loci of such functions: for instance, over the reals the polynomial $f(x_1, \ldots, x_n) := \sum x_i^2 - 1$ vanishes precisely along the unit sphere $S^{n-1} \subset \mathbb{R}^n$.

21.1.2. One should think of A as the set of "functions" on $\mathrm{Spec}(A)$ — an element $a \in A$ determines a "function" on $\mathrm{Spec}(A)$ via $\mathfrak{p} \mapsto \bar{a} \in A/\mathfrak{p}$. (For instance, the "function" $10 \in \mathbb{Z}$ determines a "function" on primes p by $p \mapsto 10 \bmod p$. This vanishes at precisely the primes dividing 10, but otherwise it doesn't make sense to ask where it takes the value $\frac{1}{9}$, for instance. It *does* in the localization $\mathbb{Z}[\frac{1}{3}]$!)

For an ideal $I \subset A$, one should think of $V(I)$ as the set of points on which functions from I vanish. One can make this more precise as follows:

Let $A = k[t_1, \ldots, t_n]$. Recall that we have a map $k^n \to \mathrm{Spec}(A)$ that attaches to $\underline{c} \in k^n$ the maximal ideal $\ker(\mathrm{ev}_{\underline{c}}) = (t_1 - c_1, \ldots, t_n - c_n)$, where

$$\mathrm{ev}_{\underline{c}} : A \to k, \quad f(t_1, \ldots, t_n) \mapsto f(\underline{c}).$$

Week 11, Problem 1. *Show that for an ideal $I \subset k[t_1, \ldots, t_n]$, the preimage of $V(I)$ under the above map $k^n \to \mathrm{Spec}(A)$ is the set*

$$\{\underline{c} \in k^n \,|\, f(\underline{c}) = 0 \,\forall f \in I\}.$$

For instance, the power of Hilbert's basis theorem is in saying that, to check whether $\underline{c}$ lies in this preimage of $V(I)$ (i.e., whether *every* function of I vanishes on $\underline{c}$), one just has to check the vanishing of *finitely many* functions.

21.1.3. Here are some basic properties of the assignment $I \rightsquigarrow V(I)$:

Lemma 21.1.4. *$V((0)) = \mathrm{Spec}(A)$; $V(A) = \emptyset$.*

Proof. Evident. □

Lemma 21.1.5. *If $I_1 \subset I_2$ then $V(I_1) \supset V(I_2)$.*

Proof. Also evident (do you see why?). □

(The point is that there are *more* conditions when saying that every element of I_2 vanishes on a point, so the vanishing locus gets smaller, yielding (a). Geometrically, if $I_1 = (f_\alpha), I_2 = (f_\alpha, g_\beta)$, then we can first see where all the f_α vanish, and then further cut out the locus of vanishing of the g_β.)

Lemma 21.1.6.

(a) *The set $V(I)$ identifies with* $\mathrm{Spec}(A/I)$.

(b) *Under the bijection of* (a)*, for another ideal $J \subset A$, the intersection $V(I) \cap V(J) \subset \mathrm{Spec}(A)$ corresponds to $V(\overline{J}) \subset \mathrm{Spec}(A/I)$, where $\overline{J}$ is the image of J under $A \to A/I =: \overline{A}$.*

Proof. Ideals in A/I are in a bijection with ideals in A containing I, and, under this bijection, prime ideals correspond to prime ideals. For part (b), $V(I) \cap V(J) = V(I + J)$, and now this follows the ideal correspondence as in (a). □

21.1.7. *Spectra and nilpotence.* We have:

Proposition 21.1.8. *$V(I) = \mathrm{Spec}(A)$ if and only if every element in I is nilpotent.*

Proof. This follows immediately from Theorem 20.2.11. □

For an ideal I, let $\sqrt{I}$ denotes its *radical*, the set

$$\{a \in A \,|\, \exists n \in \mathbb{N} \text{ such that } a^n \in I\}.$$

In other words, $\sqrt{I}$ is the preimage of the ideal of nilpotent elements under the map

$$A \to A/I.$$

For example, in $k[t]$, $\sqrt{(t^2)} = (t)$, but also $\sqrt{(t^3)} = (t)$, so don't take the notation too literally.

Lemma 21.1.9. *$V(I) = V(\sqrt{I})$.*

Proof. Combine Proposition 21.1.8 with Lemma 21.1.6. □

Proposition 21.1.10. *We have $V(I_1) \subset V(I_2)$ if and only $I_2 \subset \sqrt{I_1}$.*

Proof. The "if" direction follows from Lemmas 21.1.9 and 21.1.5. For the "only if" direction, consider the ring A/I_1, and then the assertion follows from Lemma 21.1.6(b) and Proposition 21.1.8. □

Corollary 21.1.11. *$V(I_1) = V(I_2)$ if and only if $\sqrt{I_1} = \sqrt{I_2}$.*

(What the corollary says is that while the assignment $I \rightsquigarrow V(I)$ is not an injection, i.e. you cannot recover an ideal (or just a single function) from its locus of vanishing, you can recover it up to "nilpotence". That is, $\rightsquigarrow$ is a bijection between radical ideals and $V(I)$.)

21.2. **The Zariski topology.**

21.2.1. We define a topology (called the *Zariski topology*) on $\mathrm{Spec}(A)$ as follows. Usually one declares the opens of a topology, but we will declare the closeds (which is of course equivalent by taking complements). Namely, call a subset $F \subseteq \mathrm{Spec}(A)$ closed if and only if it is of the form $V(I)$ for some I.

Let us verify that the topology axioms are satisfied. By Lemma 21.1.4, the empty set and all of $\mathrm{Spec}(A)$ are closed. Next, we have:

Lemma 21.2.2. *Let I_α be a (possibly infinite) set of ideals. Then*

$$\bigcap_\alpha V(I_\alpha) = V\left(\sum_\alpha I_\alpha\right).$$

Proof. Immediate. □

The above lemma shows that arbitrary intersections of closed subsets are closed. It remains to deal with finite unions of closeds.

21.2.3. Let I_1 and I_2 be two ideals. Consider the ideal $I_1 \cdot I_2$ *spanned* by elements

$$a_1 \cdot a_2, \quad a_i \in I_i.$$

(Note that had we taken only the set $\{a_1 \cdot a_2\}$ a priori (since we need sums to be in there too) we wouldn't have an ideal.) Note that $I_1 \supset I_1 \cdot I_2 \subset I_2$.

We claim:

Lemma 21.2.4. $V(I_1) \cup V(I_2) = V(I_1 \cdot I_2)$.

Proof. The inclusions

$$V(I_1) \subset V(I_1 \cdot I_2) \supset V(I_2)$$

are evident from Lemma 21.1.5.

For the opposite inclusion, let $\mathfrak{p} \notin V(I_1) \cup V(I_2)$. The means that there exist elements $a_1 \in I_1$ and $a_2 \in I_2$ such that $a_1, a_2 \notin \mathfrak{p}$. But then $a_1 \cdot a_2 \notin \mathfrak{p}$, since $\mathfrak{p}$ is prime. Hence, $\mathfrak{p} \notin V(I_1 \cdot I_2)$. □

Lemma 21.2.5. *We also have $V(I_1) \cup V(I_2) = V(I_1 \cap V_2)$.*

Proof. Note that

$$(I_1 \cap I_2)^2 \subset I_1 \cdot I_2 \subset I_1 \cap I_2.$$

Hence, $\sqrt{I_1 \cap I_2} = \sqrt{I_1 \cdot I_2}$. Now use Corollary 21.1.11 and Lemma 21.2.4. □

The picture here is that a union of two lines in the plane, say the x- and y-axes, is described by the vanishing of a polynomial of degree two: $xy = 0$. Note that $(x) \cdot (y) = (xy) = (x) \cap (y)$ as ideals of, say, $\mathbb{C}[x, y]$. The intersection of the two axes, however, is just a point: the origin. Note that $(x) + (y) = (x, y)$ is the ideal corresponding to the origin under our Nullstellensatz map, so everything checks out.

Week 11, Problem 2. *Show that the bijection $V(I) \simeq \mathrm{Spec}(A/I)$ of Lemma 21.1.6 is a homeomorphism, where the topology on $V(I)$ is the restriction of the Zariski topology on* $\mathrm{Spec}(A)$.

21.2.6. *Basic open subsets.* There is a wonderful coincidence that occurs in algebraic geometry that does not even come close to happening in the theory of, say, manifolds. It turns out that the complement of a very particular closed — one of the form $V(I)$ for a *principal* ideal I — is *again* of the form $\mathrm{Spec}(B)$ for some B! As we've seen all the closeds are of this form: $V(I) \simeq \mathrm{Spec}(A/I)$ — but now many opens are, too.

Namely, let $f \in A$. Let $U_f \subset \mathrm{Spec}(A)$ be the set

$$\{\mathfrak{p} \in \mathrm{Spec}(A) \mid f \notin \mathfrak{p}.\}$$

That is,

$$U_f = \mathrm{Spec}(A) - V((f)).$$

(In particular, U_f is open.)

21.2.7. Note also that U_f is empty if and only if f is nilpotent.

Lemma 21.2.8. *Let f be non-nilpotent. Then there exists a canonical bijection $U_f \simeq \mathrm{Spec}(A_f)$.*

Proof. This follows from Corollary 20.2.8. □

Week 11, Problem 3. *Show that under the bijection of Lemma 21.2.8, for an ideal $I \subset A$, the intersection $V(I) \cap U_f$ corresponds to $V(I_f) \subset \mathrm{Spec}(A_f)$.*

21.2.9. We now claim that the open subsets U_f form a basis of opens (that is, every open is a union of these "basic opens") for the Zariski topology on $\mathrm{Spec}(A)$:

Lemma 21.2.10. *Let an ideal $I \subset A$ be generated by elements $f_1, f_2, \ldots$. Then*

$$\mathrm{Spec}(A) - V(I) = \bigcup_k U_{f_k}.$$

Proof. Evident. □

Week 11, Problem 4. *Show that that the bijection $U_f \simeq \mathrm{Spec}(A_f)$ of Lemma 21.2.8 is a homeomorphism, where the topology on U_f is that induced by the Zariski topology on* $\mathrm{Spec}(A)$.

Week 11, Problem 5. *Show that the Zariski topology on* $\mathrm{Spec}(A)$*, for A a domain that is not a field, is* non-Hausdorff.

So our intuitions from topology don't work at all here.

21.2.11. *Examples.* Let A be a PID (e.g., $A = \mathbb{Z}$ or $A = k[t]$). Then A has two types of primes. One is the prime (0). Other primes are of the form $\mathfrak{p}_a := (a)$, where $a \in A$ is an irreducible element. Note that these latter primes are all maximal.

Note also that the Zariski topology on $\mathrm{Spec}(A)$ looks as follows. Apart from $\emptyset$ and $\mathrm{Spec}(A)$, the only closed subsets of $\mathrm{Spec}(A)$ are finite unions of points $\mathfrak{p}_a$. Indeed, for a closed subset $V(I)$ for $I =: (b)$, we have

$$\mathfrak{p}_a \in V(I) \Leftrightarrow a \mid b.$$

In our "elements as functions" analogy, note that these are precisely the primes for which $\overline{b} \in \mathfrak{p}$ is zero — i.e., the primes on which the "function" b vanishes.

Let us now take $A = k[t_1, t_2]$, where k is algebraically closed. Let's analyze what $\mathrm{Spec}(A)$ looks like. First, there is the element $(0) \in \mathrm{Spec}(A)$. Next, there are the

maximal ideals, which, according to the Nullstellensatz, are all of the form $\mathfrak{m}_{\underline{c}}$ for $\underline{c} \in k^n$. But there are more ideals, of course!

Since A is a UFD, any irreducible element $f \in A$ gives rise to a prime ideal — namely, (f).

Theorem 21.2.12.

(a) *Any non-zero and non-maximal prime in $k[t_1, t_2]$ is of the form (f) for a unique irreducible monic polynomial f.*

(b) *Any proper nonempty closed subset in* $\mathrm{Spec}(A)$ *is a finite union of subsets of the form $\{\mathfrak{m}_{\underline{c}}\}$ and $V((f))$, where f is irreducible.*

This will be a miniproject. But this shows the essence of what's going on. Namely, for $k = \mathbb{C}$, the vanishing locus of 0 is everything, that of $(t_1 - c_1, t_2 - c_2)$ is the point (c_1, c_2), and that of $f(t_1, t_2)$ is some one-dimensional "subvariety" (as it is called). Notice that these are all encapsulated by this spectrum formalism! So the closed subsets of $\mathbb{C}^2 \subset \mathrm{Spec}(\mathbb{C}[t_1, t_2])$ (as the maximal ideals) in this topology are precisely the vanishing loci of finitely many polynomials. Moreover, the point $(f) \in \mathrm{Spec}(\mathbb{C}[t_1, t_2])$ is not closed (its closure is $V((f))$), but the point $\mathfrak{m}_{\underline{c}} \in \mathrm{Spec}(\mathbb{C}[t_1, t_2])$ is. Finally, there are more points in the spectrum than just the points of $\mathbb{C}^2$ — that is, there are prime ideals that are not maximal — but $\mathbb{C}^2$ is precisely the set of closed points.

The collection of all points of the spectrum corresponds to the irreducible "subvarieties" of $\mathbb{C}^2$. So it stands to reason that there is a point corresponding to the whole thing itself: the prime ideal (0). Anyway, this is just for geometric motivation, and we'll make all this precise in due time.

21.3. **Irreducible decomposition.**

21.3.1. Let X be a topological space.

Definition 21.3.2. *We shall say that X is* reducible *if X can be written as $X = X_1 \cup X_2$, where $X_1, X_2 \subset X$ are proper (hence nonempty) closeds.*

For example, $V(xy)$ is the union of the x- and y-axes ($V(y)$ and $V(x)$, respectively — that is, $V(xy) = V(x) \cup V(y)$), and these are both proper closed subsets. Hence it is reducible.

Definition 21.3.3. *A topological space X is called irreducible if it is* not *reducible.*

Note that the property of irreducibility is not at all interesting for Hausdorff topological spaces:

Lemma 21.3.4. *Let X be Hausdorff and contain more than one point. Then X is reducible.*

Proof. Let $x \neq y$ be two distinct points of X. Let $x \in U, y \in V$ be disjoint opens about the points (which exist by Hausdorffness). Then $X = (X - U) \cup (X - V)$. □

However, we have:

Theorem 21.3.5. *Let A be a ring. Then* $\mathrm{Spec}(A)$ *is irreducible if and only if A/A^{nilp} has no zero-divisors (i.e., is a domain).*

Nilpotence should be thought of as "fuzz", and in our first pass through algebraic geometry we will be forgetting about any fuzz. For instance, $V(I) = V(\sqrt{I})$ — this forgets about the fact that A/I may have nilpotents, while $A/\sqrt{I}$ does not. This is why there is a condition on A/A^{nilp}, the reduced ("nonfuzzy") ring, as opposed to A itself.

Proof. By Problem 2, the map $\mathrm{Spec}(A/A^{nilp}) \to \mathrm{Spec}(A)$ is a homeomorphism, so without loss of generality A is nilpotent free. In this case $V(I) = \mathrm{Spec}(A) \Leftrightarrow I = 0$.

If A had zero divisors $fg = 0$, then $V(f) \cup V(g) = V(f \cdot g) = \mathrm{Spec}(A)$ whence $\mathrm{Spec}(A)$ is reducible.

For the converse, if we have a proper decomposition $\mathrm{Spec}(A) = V(I) \cup V(J)$, we have $V(I \cdot J) = 0$, whence $I \cdot J = 0$. Since $V(I), V(J) \subsetneq \mathrm{Spec}(A)$, $I, J \neq 0$, hence we can find $f \in I$ nonzero, and $g \in J$ nonzero. But then $fg \in I \cdot J = 0$ so $fg = 0$. □

21.3.6. We shall say that a topological space X is *Noetherian* if it does not admit infinite descending chains of closed subspaces

$$V_1 \supsetneq V_2 \supsetneq V_3 \supsetneq \cdots .$$

That is, every such chain $V_1 \supset V_2 \supset \cdots$ stabilizes (i.e., $V_k = V_\ell$ for k sufficiently large and all $\ell > k$).

Proposition 21.3.7. *Let A be a Noetherian ring. Then* $\mathrm{Spec}(A)$ *is Noetherian.*

Proof. Let

$$V_1 \supsetneq V_2 \supsetneq V_3 \supsetneq \cdots$$

be a descending chain contradicting Noetherianness. Let $V_k =: V(I_k)$. By Lemma 21.1.9, we may assume that $I_k = \sqrt{I_k}$. By Proposition 21.1.10, we have

$$I_1 \subsetneq I_2 \subsetneq I_3 \cdots ,$$

contradicting the Noetherianness of A. □

Remark 21.3.8. Note the converse is *not* true, e.g. consider

$$\mathrm{Spec}(k[x_1, x_2, x_3, \ldots]/(x_1^2, x_2^2, x_3^2, \ldots)).$$

This will be a point with "fuzz" in infinitely many directions in scheme theory — for us, it is just a point. But certainly the ring is non-Noetherian (take e.g. the non-finitely generated ideal $(x_1, x_2, x_3, \ldots)$).

We have the following general assertion:

Proposition 21.3.9. *Let X be a Noetherian topological space. Then there exists a finite decomposition*

$$X = \bigcup_{i=1}^{n} X_k,$$

where each X_k is closed in X and irreducible *as a topological space.*

That is, every Noetherian topological space can be decomposed into (finitely many!) irreducible components.

Proof. Suppose that such a decomposition does not exist; in particular X is *reducible*. Write

$$X = X_1 \cup X_2,$$

where X_1 and X_2 are closed and neither equals all of X. If both X_1 and X_2 admit a decomposition as in the proposition, this would be a contradiction (concatenate the decompositions). So without loss of generality X_1 does not admit one. Set $V_1 := X_1$. Now, continue the process. We obtain a descending chain

$$V_1 \supsetneq V_2 \supsetneq V_3 \supsetneq \cdots,$$

contradicting the assumption that X was Noetherian. □

21.3.10. We shall say that a prime ideal $\mathfrak{p}$ in a ring A is *minimal* if it is minimal with respect to inclusions among primes. That is, there is no $\mathfrak{q}$ prime such that $\mathfrak{q} \subsetneq \mathfrak{p}$.

Theorem 21.3.11. *Let A be Noetherian. Then A contains a finite number of minimal primes. Moreover, any prime ideal of A contains a minimal prime.*

Proof. Let

$$\mathrm{Spec}(A) = \bigcup_{i=1}^{n} V(I_k)$$

be a decomposition of $\mathrm{Spec}(A)$ into irreducibles given by Proposition 21.3.9. With no restriction of generality we can assume that this decomposition is irredundant, i.e., no $V(I_k)$ is properly contained in any other $V(I_{k'})$ (otherwise, just leave it out!).

Further, by Lemma 21.1.9, we can assume that $I_k = \sqrt{I_k}$ — i.e., that the rings A/I_k have no nilpotents.

By Problem 2, $\mathrm{Spec}(A/I_k)$ is irreducible. Hence, by Theorem 21.3.5, the ring A/I_k has no zero divisors. Hence each I_k is prime; write now $\mathfrak{p}_k := I_k$ instead. We claim that the resulting primes

$$\mathfrak{p}_1, \ldots, \mathfrak{p}_n$$

are the minimal primes of A.

The inclusion $\mathrm{Spec}(A) \subset \bigcup_{i=1}^{n} V(\mathfrak{p}_k)$ means that any prime ideal $\mathfrak{p}$ contains one of the $\mathfrak{p}_k$'s.

Now, if $\mathfrak{p} \subsetneq \mathfrak{p}_k$, the for some k' we have

$$\mathfrak{p}_{k'} \subset \mathfrak{p} \subsetneq \mathfrak{p}_k \Rightarrow V(I_k) \subsetneq V(I_{k'}),$$

which is a contradiction to our assumption that the list was not redundant. □

Remark 21.3.12. The fact that any prime ideal contains a minimal prime is valid for *any* A (no need for the Noetherian assumption), but the proof uses Zorn's lemma. (Do it! The only difference is the decomposition into irreducible components. If you get stuck, look up *König's Lemma*.)

Note that the definition of minimal prime did not involve the choice of an irreducible decomposition. Hence the decomposition is in fact canonical. Anyway, we may speak of "the" minimal primes of A rather than a choice of minimal primes of A.

Proposition 21.3.13. *Let A be a Noetherian ring and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be its minimal primes.*

(a) *The containment*

$$\bigcup_{k \neq k_0} V(\mathfrak{p}_k) \subset \mathrm{Spec}(A)$$

is proper.

(b) *The map*

$$A/A^{nilp} \to \prod_{k=1}^{n} A/\mathfrak{p}_k$$

is injective.

Another way to phrase the second part is as follows. The ideal of nilpotents is the intersection of *all* prime ideals of A. The second part says that the intersection only has to be taken over the finitely many minimal primes. (It should now be clear how the proof will go!)

Proof. For (a), we claim that the prime $\mathfrak{p}_{k_0} \in \mathrm{Spec}(A)$ is not contained in the union

$$\bigcup_{k \neq k_0} V(\mathfrak{p}_k).$$

Indeed, if $\mathfrak{p}_{k_0} \in V(\mathfrak{p}_k)$, then $\mathfrak{p}_k \subset \mathfrak{p}_{k_0}$, contradicting the minimality assumption on $\mathfrak{p}_{k_0}$.

For (b), we need to show that

$$\ker(A \to \prod_{k=1}^{n} A/\mathfrak{p}_k)$$

consists only of nilpotent elements. However, by Theorem 21.3.11, if $a \in A$ belongs to the above kernel, it belongs to *any* prime ideal of A. Hence, it is nilpotent. □

21.4. **Supports of modules.**

21.4.1. Let M be an A-module. We define $\mathrm{supp}(M) \subset \mathrm{Spec}(A)$ to be the set

$$\mathrm{supp}(M) := \{\mathfrak{p} \mid M_{\mathfrak{p}} \neq 0\},$$

where $M_{\mathfrak{p}}$ is the localization of M at $\mathfrak{p}$ — i.e., with respect to the multiplicative set $A - \mathfrak{p}$.

21.4.2. Now for some structural properties.

Lemma 21.4.3. *Let*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

be a short exact sequence. Then

$$\mathrm{supp}(M_2) = \mathrm{supp}(M_1) \cup \mathrm{supp}(M_3).$$

Proof. By Proposition 20.4.8, for a prime $\mathfrak{p}$, we have a short exact sequence

$$0 \to (M_1)_{\mathfrak{p}} \to (M_2)_{\mathfrak{p}} \to (M_3)_{\mathfrak{p}} \to 0,$$

and the assertion follows. □

21.4.4. We now claim:

Proposition 21.4.5. *Let $M \neq 0$. Then* $\mathrm{supp}(M) \neq \emptyset$.

Proof. Let $m \in M$ be a nonzero element. Then it defines an injection

$$A/I \hookrightarrow M, \quad a \mapsto a \cdot m,$$

where $I = \mathrm{Ann}_A(m)$, the annihilator of m. Note that $I \neq A$ since $m = 1 \cdot m \neq 0$.

Hence, by Lemma 21.4.3, we can assume that $M = A/I$ as an A-module.

Let $\overline{\mathfrak{p}}$ be any prime in $\overline{A} := A/I$. Then $\overline{A}_{\overline{\mathfrak{p}}} \neq 0$ (do you see why?). Let $\mathfrak{p}$ be the preimage of $\mathfrak{p}$ under $A \to \overline{A}$. We claim that $(A/I)_{\mathfrak{p}} \neq 0$. This follows from the next general assertion:

Lemma 21.4.6. *Let N be an A/I-module, and $S \subset A$ a multiplicative set such that $S \cap I = \emptyset$. Let $\overline{S}$ be the projection of S under $A \to A/I =: \overline{A}$. Then $N_S \simeq N_{\overline{S}}$.*

Proof. Do it yourself! □

□

22. Thursday, April 18

22.1. **Support of modules, continued.**

22.1.1. Let $I \subset A$ be an ideal and consider the ring $\overline{A} := A/I$. Let M be a module over $\overline{A}$, which we can also consider as a module over A via the projection $A \to \overline{A}$.

Proposition 22.1.2. *The support of M, considered as an A-module, is contained in $V(I)$. Moreover, under the identification $V(I) \simeq \mathrm{Spec}(\overline{A})$, the support of M as an A module goes over to the support of M as an $\overline{A}$-module.*

Proof. To prove that $\mathrm{supp}(M) \subset V(I)$, it is enough to show that if a multiplicative set S is such that $S \cap I \neq \emptyset$, then $M_S = 0$, which is immediate from the fact that I acts on M by 0:

$$\frac{m}{s} = \frac{f \cdot m}{f \cdot s}, \quad f \in S,$$

and the right-hand side equals zero if $f \in I$.

The second assertion follows from Lemma 21.4.6.

□

22.1.3. Let $S \subset A$ be a multiplicative set. For an A-module M, consider the A_S-module M_S. Recall also that $\mathrm{Spec}(A_S)$ is naturally a subset of $\mathrm{Spec}(A)$ — see Corollary 20.2.8.

Proposition 22.1.4. *The support of M_S as an A_S-module equals*

$$\mathrm{supp}(M) \cap \mathrm{Spec}(A_S).$$

Week 11, Problem 6. *Prove Proposition 22.1.4.*

22.1.5. For future reference, we note the following:

Proposition 22.1.6. *Let $T : M \to N$ be a map of A-modules. Then T is an injection/surjection/isomorphism if and only if for every prime $\mathfrak{p} \in \mathrm{Spec}(A)$, the induced map*

$$T_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$$

is an injection/surjection/isomorphism.

What this is saying is that, to check injectivity or surjectivity, it suffices to check "locally" — i.e., upon localizing at a prime (so that now one has a unique maximal ideal).

Proof. Let us prove the statement regarding injections (the case of surjections is similar). Set $K := \ker(T)$. From Proposition 20.4.8, we obtain that

$$K_{\mathfrak{p}} \simeq \ker(T_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}).$$

So, clearly, if $K = 0$, then $T_{\mathfrak{p}}$ is injective for any $\mathfrak{p}$. Conversely, if $T_{\mathfrak{p}}$ is injective for any $\mathfrak{p}$, we obtain that $K_{\mathfrak{p}} = 0$ for all $\mathfrak{p}$, hence $\mathrm{supp}(K) = \emptyset$ — hence $K = 0$ by Proposition 21.4.5.

□

Week 11, Problem 7. *Let $f_1, \ldots, f_n$ be elements of A such that*

$$\bigcup_i U_{f_i} = \mathrm{Spec}(A),$$

where $U_f := \mathrm{Spec}(A_f)$ as usual. Let $T : M \to N$ be a map such that the maps $T_{f_i} : M_{f_i} \to N_{f_i}$ are injections/surjections/isomorphisms for all $i = 1, \ldots, n$. Show that T is then an injection/surjection/isomorphism.

22.2. **Closed subsets containing the support.**

22.2.1. We are going to prove:

Theorem 22.2.2. *For an A-module M and an ideal $I \subset A$, the support of M is contained in $V(I)$ if and only if every element of I acts* locally nilpotently *on M — i.e., for every $f \in I$ and $m \in M$, there exists a power n such that $f^n \cdot m = 0$.*

(Note that to say that f acts nilpotently would be to say that f^n acts by zero on M. That is, the n above is allowed to depend on f *and* m, whence "locally".)

Proof. Suppose first that every element of I acts locally nilpotently on M. Let us show that $\mathrm{supp}(M) \subset V(I)$. That is, we need to show that, for any $\mathfrak{p} \in \mathrm{Spec}(A)$ with $\mathfrak{p} \notin V(I)$, we have $M_{\mathfrak{p}} = 0$.

The condition that $\mathfrak{p} \notin V(I)$ means that there exists $f \in I \cap (A - \mathfrak{p})$. In this case for any element $\frac{m}{a} \in M_{\mathfrak{p}}$, we have

$$\frac{m}{a} = \frac{f^n \cdot m}{f^n \cdot s} = 0.$$

Let now f be an element of I, and suppose that it does *not* act locally nilpotently. Thie means that there exists $m \in M$ such that none of the elements $f^n \cdot m$ are zero. Consider the A_f-module M_f. By assumption, the element $\frac{m}{1} \in M_f$ is nonzero. In particular, $M_f \neq 0$. By Proposition 22.1.4, we obtain

$$\mathrm{supp}(M) \cap U_f \neq \emptyset.$$

Since $U_f \cap V(I) = \emptyset$, this implies that $\mathrm{supp}(M)$ is not contained in $V(I)$.

□

22.2.3. We will now prove a more precise version of Theorem 22.2.2. For a module M, let $\mathrm{Ann}(M)$ denote its annihilator, i.e., the set of all

$$\{f \in A \,|\, f \cdot m = 0 \ \forall m \in M\}.$$

Theorem 22.2.4. *Let M be finitely generated. Then $\mathrm{supp}(M) = V(I)$, where $I = \mathrm{Ann}(M)$.*

Proof. The containment $\mathrm{supp}(M) \subset V(\mathrm{Ann}(M))$ follows from Theorem 22.2.2. Let us show that if $\mathfrak{p} \notin \mathrm{supp}(M)$, then $\mathfrak{p} \notin V(I)$.

Let $m_1, \ldots, m_n$ be a generating set of M. If $\mathfrak{p}$ is such that $M_\mathfrak{p} = 0$, then, for each i, the element $\frac{m_i}{1} \in M_\mathfrak{p}$ is zero. I.e., there exists $f_i \in A - \mathfrak{p}$ such that $f_i \cdot m_i = 0$. Let

$$f := \prod_{i=1}^{n} f_i.$$

The element f annihilates all the generators of M and hence belongs to $\mathrm{Ann}(M)$. On the other hand, since $\mathfrak{p}$ is prime, $f \notin \mathfrak{p}$. Hence $\mathrm{Ann}(M)$ isn't contained in $\mathfrak{p}$. So $\mathfrak{p} \notin V(I)$.

□

22.2.5. Notice how crucially we used the finite generation hypothesis! The assumption that M be finitely generated in Theorem 22.2.4 is in fact essential. For example, take $A := k[t]$, and let M be the A-module $k[t, t^{-1}]/k[t]$. (Do you see why this is not finitely generated as an A-module?)

Week 11, Problem 8. *Calculate* $\mathrm{supp}(M)$ *and* $\mathrm{Ann}(M)$. *Show that* $\mathrm{supp}(M) \neq V(\mathrm{Ann}(M))$.

22.2.6. We will now prove the following basic result:

Theorem 22.2.7. *Let $V_1, V_2 \subset \mathrm{Spec}(A)$ be two closed subsets such that $V_1 \cap V_2 = \emptyset$.*
(a) *If $\mathrm{supp}(M_i) \subset V_i$, then $\mathrm{Hom}(M_1, M_2) = 0$.*
(b) *Let M be an A-module such that $\mathrm{supp}(M) \subset V_1 \cup V_2$. Then $M = M_1 \oplus M_2$ for some M_i such that $\mathrm{supp}(M_i) \subset V_i$.*

Proof. For point (a), let T be a morphism $M_1 \to M_2$, and let N be its image. Then $M_1 \to N$ is surjective. Of course $\mathrm{supp}(N) \subset \mathrm{supp}(M_2) \subset V_2$ (since if $N_\mathfrak{p} \neq 0$, then $N \subset M_2$ implies $(M_2)_\mathfrak{p} \neq 0$). But if $\mathfrak{p} \in V_2$, then $(M_1)_\mathfrak{p} = 0$, whence the surjection $(M_1)_\mathfrak{p} \to N_\mathfrak{p}$ tells us that $N_\mathfrak{p} = 0$. So N has no support, whence $N = 0$.

For point (b), let $V_i =: V(I_i)$. The assumption that $V_1 \cap V_2 = \emptyset$ means that $I_1 + I_2 = A$. I.e., there exist elements $f_1 \in I_1$ and $f_2 \in I_2$ such that $f_1 + f_2 = 1$. Let $J_i := (f_i)$. We have

$$V(I_i) \subset V(J_i) \text{ and } V(J_1) \cap V(J_2) = \emptyset.$$

Set

$$M_1 := \{m \in M \,|\, \exists n \in \mathbb{N} \ f_1^n \cdot m = 0\} \text{ and } M_2 := \{m \in M \,|\, \exists n \in \mathbb{N} \ f_2^n \cdot m = 0\}.$$

By Theorem 22.2.2, we have $\mathrm{supp}(M_1) \subset V(J_1) \cap (V(I_1) \cup V(I_2))$. Since

$$V(J_1) \cap V(I_2) \subset V(J_1) \cap V(J_2) = \emptyset,$$

we conclude that $\mathrm{supp}(M_1) \subset V(I_1)$. Similarly, $\mathrm{supp}(M_2) \subset V_2$.

Now consider the map $M_1 \oplus M_2 \to M$. The kernel is $M_1 \cap M_2$, which has support contained in both V_1 and V_2 (since $M_1 \cap M_2$ is contained in M_1 and M_2), whence it has empty support, whence it is zero. So the map is injective. It remains to show that every element $m \in M$ can be written as $m_1 + m_2$ with $m_i \in M_i$ (i.e., that the map is surjective).

So let $m \in M$. Since $\mathrm{supp}(M) \subset V(I_1) \cup V(I_2) = V(I_1 \cdot V_2)$, by Theorem 22.2.2, the element $f_1 \cdot f_2$ acts locally nilpotently on M. I.e., there exists an integer n (depending on $f_1 \cdot f_2$ and m) such that $(f_1 \cdot f_2)^n \cdot m = 0$.

But

$$\begin{aligned} m &= (f_1 + f_2)^{2n} \cdot m \\ &= \left(\sum_{k=0}^{n} \binom{2n}{k} (f_1^k \cdot f_2^{n-k})(f_2^n m) \right) + \left(\sum_{k=0}^{n} \binom{2n}{n-k} (f_1^k \cdot f_2^{n-k})(f_1^n m) \right) \end{aligned}$$

by the binomial theorem and the fact that $f_1 + f_2 = 1$ (do you see why?). But now notice that the first term in parentheses is in M_1, since multiplying by f_1^n gives

$$\sum_{k=0}^{n} (\cdots)\, ((f_1 \cdot f_2)^n m) = 0.$$

Similarly the second term is in M_2. This completes the proof. □

22.3. **Artinian rings.**

22.3.1. We will prove the following basic result:

Theorem 22.3.2. *Let A be a Noetherian ring. The following conditions are equivalent:*

(a) *A is of finite length as a module over itself.*

(b) *Every prime ideal in A is maximal.*

(c) *$A \simeq \bigoplus_{i=1}^{n} A_i$, where each A_i is a local ring such that every element in its maximal ideal is nilpotent.*

Rings satisfying the equivalent conditions of Theorem 22.3.2 are called *Artinian*.

Proof. Let us assume (a) and deduce (b). Let $\mathfrak{p} \subset A$ be a prime. We need to show that $A/\mathfrak{p}$ is a field. I.e., that any $0 \neq f \in A/\mathfrak{p}$ is invertible.

Since A is of finite length as an A-module, the same is true for any of its quotients. Hence, $A/\mathfrak{p}$ is of finite length as a module over A, and hence so as a module over itself. Hence, any chain of $A/\mathfrak{p}$-submodules of $A/\mathfrak{p}$ has length bounded by the length of $A/\mathfrak{p}$.

Consider the ideals

$$A \supset (f) \supset (f^2) \supset (f^3) \supset \cdots .$$

We obtain that there exists n such that

$$(f^n) = (f^{n+1}).$$

I.e., there exists $g \in A/\mathfrak{p}$ such that $g \cdot f^{n+1} = f^n$. I.e., $f^n(f \cdot g - 1) = 0$. But $A/\mathfrak{p}$ is a domain ($\mathfrak{p}$ was prime), so we obtain that $f \cdot g = 1$, as required.

Let us assume (b) and deduce (c). Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the minimal primes of A (there are finitely many of them by Theorem 21.3.11). Note that, by assumption, these are *all* the primes of A. Set $A_i := A_{\mathfrak{p}_i}$. This is a local ring by Proposition 20.3.6. Moreover, by Corollary 20.2.8, the maximal ideal in A_i is its only prime. Hence, every element of this maximal ideal is nilpotent by Corollary 20.2.12.

Let us show that the map

$$A \to \bigoplus_{i=1}^{n} A_i$$

is an isomorphism. By Proposition 22.1.6, it is sufficient to show that for every prime $\mathfrak{p}$, the map

$$A_{\mathfrak{p}} \to \bigoplus_{i=1}^{n} (A_i)_{\mathfrak{p}}$$

is an isomorphism. We claim that $(A_i)_{\mathfrak{p}} = 0$ for $\mathfrak{p} \neq \mathfrak{p}_i$ and $(A_i)_{\mathfrak{p}} \simeq A_i$ if $\mathfrak{p} = \mathfrak{p}_i$.

Since every element of $\mathfrak{p}_i$ is nilpotent when mapped to A_i, from Theorem 22.2.2, we obtain that the support of A_i (viewed as an A-module) is contained in the singleton

$$\{\mathfrak{p}_i\} \subset \mathrm{Spec}(A).$$

This shows that $(A_i)_{\mathfrak{p}} = 0$ for $\mathfrak{p} \neq \mathfrak{p}_i$.

The fact that $(A_{\mathfrak{p}_i})_{\mathfrak{p}_i} \simeq A_{\mathfrak{p}_i}$ is evident: for any multiplicative set S and any module M, the map

$$M_S \to (M_S)_S$$

is an isomorphism (do you see why?).

Finally, let us assume (c) and deduce (a). We may assume that A equals one of the A_i's. I.e., we may assume that A is a local Noetherian ring with (unique) maximal ideal $\mathfrak{m}$, in which every element of $\mathfrak{m}$ is nilpotent.

Let $f_1, \ldots, f_n$ be generators of $\mathfrak{m}$. By assumption, there exists an integer N such that $f_i^N = 0$ for each i. Hence, by the binomial formula, $\mathfrak{m}^{n \cdot N} = 0$. Consider the sequence of submodules

$$A \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \cdots .$$

By the above, this chain is finite. It remains to show that each $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ has finite length. Note that the action of A on $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ factors through $A/\mathfrak{m}$, and the latter is a field. Hence, it is enough to show that $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is finitely generated. This, in turn, follows from the fact that $\mathfrak{m}^i$ is so (by the i-fold products of the n generators).

□

22.3.3. Note that the implication (a) ⇒ (c) in Theorem 22.3.2 gives an alternative proof of Theorem 13.2.5. We will now prove:

Proposition 22.3.4. *Let k be an algebraically closed field, and let A be a finitely-generated k-algebra which is Artinian. Then A is finite-dimensional as a k-vector space.*

Week 11, Problem 9. *Deduce Proposition 22.3.4 from Problem 5, Week 10.*

In addition, we also have the following:

Theorem 22.3.5. *Let k be an algebraically closed field, and let A be a finitely-generated k-algebra. Assume that A has only finitely many* maximal *ideals. Then A is finite-dimensional as a k-vector space.*

Week 11, Optional problem, 2pts. *Prove Theorem 22.3.5.*

Suggested strategy: Let $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ be the maximal ideals of A. (a) Show that one can find elements $f_1, \dots, f_n \in A$ such that $f_i \notin \mathfrak{m}_i$ but $f_i \in \mathfrak{m}_j$ for all $j \neq i$. (b) Show that the basic opens U_{f_i} cover $\mathrm{Spec}(A)$. (c) Use the Nullstellensatz to show that $(\mathfrak{m}_i)_{f_i}$ is the unique prime in A_{f_i}.

22.4. **Modules over Artinian rings.**

22.4.1. Let A be a Noetherian ring, and let M be a finitely generated A-module. We will prove:

Theorem 22.4.2. *The following conditions are equivalent:*

(a) *M is of finite length.*

(b) *The ring $A/\operatorname{Ann}(M)$ is Artinian.*

(c) $\operatorname{supp}(M)$ *is a finite union of maximal ideals.*

Proof. Let us assume (a) and deduce (b). Let $m_1, \dots, m_n$ be a generating set of M. Consider the map

$$A \to \bigoplus_{i=1}^{n} M, \quad 1 \mapsto (m_1, \dots, m_n).$$

This map factors through an *injection*

$$A/\operatorname{Ann}(M) \to \bigoplus_{i=1}^{n} M.$$

Hence, if M has a finite length as an A-module, then so does $A/\operatorname{Ann}(M)$. But that is the same as $A/\operatorname{Ann}(M)$ having a finite length as a module over itself.

That (b) implies (c) follows immediately from Proposition 22.1.2.

Week 11, Problem 10. *Now prove (c) $\Rightarrow$ (a).*

□

23. Tuesday, April 23

23.1. **Finitely presented modules.**

Definition 23.1.1. *An A-module M is said to be* finitely presented *if it can be exhibited as a quotient of $A^{\oplus n}$ by a* finitely generated *submodule.*

Note that for Noetherian rings, there is no difference between "finitely generated" and "finitely presented." The reason for the name is that such a module can be *presented* as $M \simeq \langle m_1, \dots, m_n | r_1, \dots, r_k \rangle$ for m_i a finite set of generators and r_i a finite set of relations (i.e., generators of the kernel). That is, such a thing admits a finite presentation.

Proposition 23.1.2. *Let M be finitely presented, and let $\alpha : N \to M$ be a surjection, where N is finitely generated. Then* $\ker(\alpha)$ *is finitely generated.*

Proof. Let $P := A^{\oplus n}$ be such that there exists a surjection $\beta : P \to M$ with a finitelt generated kernel. Consider the module $Q := P \oplus N$ and the map

$$\gamma := (\beta + \alpha) : Q \to M.$$

Note that we have a short exact sequence

$$0 \to \ker(\beta) \to \ker(\gamma) \to N \to 0.$$

Hence, $\ker(\gamma)$ is finitely generated. Note that we also have a short exact sequence

$$0 \to \ker(\alpha) \to \ker(\gamma) \to P \to 0. \tag{23.1}$$

We will show that $\ker(\alpha)$ is finitely generated by showing that the short exact sequence (23.1) splits.

Since P is free and α is a surjection, we can find a map $\delta : P \to N$ such that $\alpha \circ \delta = \beta$ (pick where the generators go). The map δ gives rise to a map

$$\epsilon := (\mathrm{id}, -\delta) : P \to Q,$$

whose image belongs to $\ker(\gamma)$. The datum of the above map $\epsilon : P \to \ker(\gamma)$ defines a splitting of (23.1).

□

Week 12, Problem 1. *Let us be in the setting of Problem 7, Week 11. Show that if M is such that each M_{f_i} is finitely generated/presented module over A_{f_i}, then M itself is finitely generated/presented.*

23.2. **More on support and localization.**

Week 12, Problem 2. *Let M be a finitely generated A-module. Let $\mathfrak{p} \notin \mathrm{supp}(M)$. Show that there exists $f \in A$ with $\mathfrak{p} \in U_f$ such that $M_f = 0$.*

23.3. **Decomposition of modules with disjoint support, an addendum.** Let us be in the situation of Theorem 22.2.7:

Proposition 23.3.1. *The submodule M_1 equals*

$$M_1' := \{m \in M \,|\, \forall f_1 \in I_1 \ \exists n \text{ such that } f_1^n \cdot m = 0.\}$$

Proof. The fact that $M_1 \subset M_1'$ follows from Theorem 22.2.2. To show the converse inclusion, it suffices to show that $M_1' \cap M_2 = 0$. Choose $f_1 \in I_1$ and $f_2 \in I_2$ such that $f_1 + f_2 = 1$. We claim that the element f_1 does not act locally nilpotently on *any* submodule of M_2. In fact, we claim that f_1 acts invertibly on M_2. Indeed, its inverse is given by the sum

$$1 + f_2 + f_2^2 + \cdots,$$

which makes sense because f_2 acts locally nilpotently on M_2 (do you see why?).

□

23.4. **Artinian rings and modules over them.**

23.4.1. Let us give an alternative proof for (b) $\Rightarrow$ (c) in Theorem 22.3.2.

Note that the assumption in (b) combined with Theorem 21.3.11 implies that $\mathrm{Spec}(A)$ is the disjoint union of the elements $\{\mathfrak{m}_i\}$, where $\mathfrak{m}_i$ are the primes of A (note that the primes of A are also all minimal primes, as well as maximal ideals).

By Theorem 22.2.7, applied to $M = A$, we can write

$$A = J_1 \oplus \cdots \oplus J_n,$$

where $J_i \subset A$ are ideals and $\mathrm{supp}(J_i) \subset \{\mathfrak{m}_i\}$.

This gives a decomposition of A as a direct sum of rings

$$A = A_1 \oplus \cdots \oplus A_n.$$

Let us prove that each A_i is local, and such that every element in its maximal ideal is nilpotent. Let us view A_i as a quotient ring of A. The fact that $\mathrm{Spec}(A_i)$ consists of one point follows from Proposition 22.1.2: indeed $\mathrm{Spec}(A_i)$ equals the support of A_i as an A_i-module, which equals the support of A_i as an A-module, and the latter equals $\{\mathfrak{m}_i\}$, by construction. Hence, A_i has a unique prime ideal. In particular, this prime is the unique maximal ideal. Every element in it is nilpotent by Corollary 20.2.12.

Note that if $\overline{\mathfrak{m}}_i$ denotes the (unique) maximal ideal in A_i, its preimage in A is the corresponding maximal ideal $\mathfrak{m}_i$. In terms of the direct sum decomposition

$$\mathfrak{m}_i = \left(\bigoplus_{j \neq i} A_j\right) \bigoplus \overline{\mathfrak{m}}_i.$$

23.4.2. Let us now show that A_i identifies with the localization $A_{\mathfrak{m}_i}$. In fact, we claim that the canonical map $A \to A_{\mathfrak{m}_i}$ factors as

$$A \twoheadrightarrow A_i \to A_{\mathfrak{m}_i},$$

where the second arrow is an isomorphism.

Indeed, the factorization follows from the fact that for $j \neq i$ we have $(A_j)_{\mathfrak{m}_i} = 0$ (the latter because $\mathrm{supp}(A_j) \subset \{\mathfrak{m}_j\}$, by construction).

Hence, it remains to show that the map $A_i \to (A_i)_{\mathfrak{m}_i}$ is an isomorphism. Note that by Lemma 21.4.6, $(A_i)_{\mathfrak{m}_i} \simeq (A_i)_{\overline{\mathfrak{m}}_i}$. Now the assertion follows from the fact that A_i is a local ring:

For any local ring A' with maximal ideal $\mathfrak{m}'$, the map $A' \to A'_{\mathfrak{m}'}$ is an isomorphism because the set $A' - \mathfrak{m}'$ consists of invertible elements (see Lemma 20.3.2).

23.4.3. Let now M be an A-module.

Note that if R is a ring, written as $R_1 \oplus R_2$, then any R-module M canonically splits as a direct sum $M_1 \oplus M_2$, where R acts on M_i via first projecting $R \twoheadrightarrow R_i$ (that is, R_2 acts trivially on M_1, and vice versa). Indeed, let 1_1 and 1_2 be the units in R_1 and R_2, respectively. Then the actions of 1_1 and 1_2 on M are idempotents (i.e., they square to themselves, like projection operators in linear algebra), and

$$\mathrm{Im}(1_1 \cdot -) \oplus \mathrm{Im}(1_2 \cdot -)$$

is the desired decomposition.

Iterating, we obtain that M splits as a direct sum of modules

$$M_1 \oplus \cdots \oplus M_n,$$

where A acts on M_i via the projection $A \to A_i$.

We claim:

Proposition 23.4.4.

(a) $\mathrm{supp}(M_i) \subset \{\mathfrak{m}_i\}$, *so* $M = M_1 \oplus \cdots \oplus M_n$ *coincides with the decomposition of Theorem 22.2.7.*

(b) *The map* $M \to M_{\mathfrak{m}_i}$ *factors as* $M \to M_i \to M_{\mathfrak{m}_i}$, *where the second arrow is an isomorphism.*

Proof. Point (a) follows from Proposition 22.1.2. Point (b) repeats the proof in Sect. 23.4.2.

Alternatively, we can view the decomposition $M = M_1 \oplus \cdots \oplus M_n$ as coming from

$$M \simeq A \underset{A}{\otimes} M \simeq (A_1 \oplus \cdots \oplus A_n) \underset{A}{\otimes} M \simeq (A_1 \underset{A}{\otimes} M) \oplus \cdots \oplus (A_n \underset{A}{\otimes} M).$$

Now use the the isomorphism $A_i \to A_{\mathfrak{m}_i}$ and

$$M_{\mathfrak{m}_i} \simeq A_{\mathfrak{m}_i} \underset{A}{\otimes} M$$

of Proposition 20.4.6.

□

Corollary 23.4.5. *For* $M = M_1 \oplus \cdots \oplus M_n$ *as above, we have:*

$$M_i = \{m \in M \,|\, \forall f_i \in \mathfrak{m}_i \ \exists n \text{ such that } f_i^n \cdot m = 0\},$$

and $A - \mathfrak{m}_i$ *acts on* M_i *invertibly.*

Proof. The first assertion follows from Propositions 23.4.4(a) and 23.3.1. The second assertion follows from Proposition 23.4.4(b). □

23.4.6. *Example.* Take $A = \mathbb{Z}/n\mathbb{Z}$ for a nonzero integer n.

Write $n = \prod_p p^{m_p}$, where p's are prime numbers. In this case, Proposition 23.4.4 says that any abelian group M, in which every element to the power n equals zero, can be written as a direct sum

$$M \simeq \bigoplus_p M_p,$$

such that in M_p every element to the power p^{m_p} equals zero.

Let r_p be any element in $\mathbb{Z}$ that projects under $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} = A$ to the unit $1_p \in A_p \subset A$. We obtain that the action of r_p on M (i.e., raising to the power r_p) is the projection onto the M_p-direct summand.

When M is finite, this is the familiar result from the classification of finite abelian groups.

23.4.7. *Another example.* Take $A = k[t]/(p(t))$, where k is algebraically closed. Write $p(t) =: \prod_i (t-\lambda_i)^{m_i}$. Let M be an A-module. In particular, M is a module over $k[t]$. I.e., we can think of M as a k-vector space V equipped with a linear operator T such that $p(T) = 0$ as linear operators. Assume that V is finite-dimensional.

The assumption that the action of $k[t]$ on M factors through an action of $A = k[t]/p(t)$ is equivalent to the fact that $\min_T(t)|p(t)$.

Now, Proposition 23.4.4 says that we can write V as a direct sum

$$V \simeq \bigoplus_i V_i,$$

such that $T - \lambda_i$ acts nilpotently on V_i. I.e., V_i is the λ_i-generalized eigenspace.

Let $r_i(t) \in k[t]$ be any element that projects under $k[t] \to k[t]/p(t) = A$ to the unit $1_i \in A_i \subset A$. We obtain that the action of $r_i(T)$ defines the projection of V into V_i.

23.5. **Dimension of rings.**

23.5.1. Let A be a commutative Noetherian ring. Its (Krull) dimension is the supremum of the lengths n (*not* $n+1$!) of chains of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{n-1} \subsetneq \mathfrak{p}_n.$$

Intuitively, it is the longest chain of proper irreducible subvarieties that the space admits. For instance, a closed submanifold of $\mathbb{R}^n$ is either the whole thing or of dimension strictly smaller than n (this is nontrivial already! — it is called "invariance of domain"). The process continues: irreducibility corresponds to connectedness, and a proper closed submanifold of a connected manifold is necessarily of smaller dimension, thanks to this "invariance of domain" (which uses Brouwer's fixed point theorem). But of course $\mathbb{R}^n$ admits a chain of length n: $\mathbb{R}^n \supsetneq \mathbb{R}^{n-1} \supsetneq \cdots \supsetneq \mathbb{R}^0 = \mathrm{pt}$, so it has dimension n in the analogous definition.

For another example, $\dim_{\mathrm{Krull}}(A) = 0$ if and only if A is Artinian. That is, Artinian rings correspond to collections of (potentially fuzzy) points. As in manifold theory, we next turn to the study of one-dimensional objects (recall that in manifold theory that one-manifolds are collections of circles and (open, closed, or clopen) intervals, and that this classification is extremely useful in the higher-dimensional theory).

23.5.2. *Domains of dimension one.* Let A be a domain, so that (0) is its (only) minimal prime. The following follows immediately from the definition:

Lemma 23.5.3. $\dim_{\mathrm{Krull}}(A) = 1$ *if and only if every nonzero prime is maximal.*

In particular:

Corollary 23.5.4. *Let A be a PID. Then* $\dim_{\mathrm{Krull}}(A) = 1$.

For future use, let us note the following:

Lemma 23.5.5. *If* $\dim_{\mathrm{Krull}}(A) = 1$*, then any* proper *quotient of A is Artinian.*

Proof. If $\overline{A} \twoheadleftarrow A$ is a proper quotient of A, and if $\overline{\mathfrak{p}} \subset \overline{A}$ is a prime, then its preimage $\mathfrak{p}$ in A is a nonzero prime, and hence is maximal. Hence, $\overline{\mathfrak{p}}$ is maximal, too. □

Corollary 23.5.6. *Any non-empty proper closed subset of* $\mathrm{Spec}(A)$ *is the union of finitely many* closed *points.*

Note that for any ring A, a point $\mathfrak{p} \in \mathrm{Spec}(A)$ is closed as a subset of $\mathrm{Spec}(A)$ if and only if $\mathfrak{p}$ is maximal (indeed, the closure of $\{\mathfrak{p}\}$ is $V(\mathfrak{p})$, the set of primes containing $\mathfrak{p}$).

23.5.7. As a mini-project we will prove:

Theorem 23.5.8. *Let k be a field. Then the* $\dim_{\mathrm{Krull}}(k[t_1, \ldots, t_n]) = n$.

You should expect this because $\mathbb{C}^n$ is an n-dimensional complex manifold, and the Nullstellensatz says that the closed points of $\mathbb{C}[t_1, \ldots, t_n]$ are precisely the points of $\mathbb{C}^n$, but it is highly nontrivial to prove.

Let us see what it says for $n = 2$:

Corollary 23.5.9. *Any non-zero and non-maximal prime in $k[x, y]$ is of the form (f) for an irreducible polynomial $f \in k[x, y]$.*

Proof. Let $\mathfrak{p}$ be a nonzero and nonmaximal prime. Take any nonzero element $f \in \mathfrak{p}$, and decompose it into irreducibles

$$f = f_1 \cdots f_n.$$

Since $\mathfrak{p}$ is prime, we have $f_i \in \mathfrak{p}$ for at least one i. Since $k[x, y]$ is a UFD, we obtain that (f_i) is prime. Thus, we have

$$(0) \subsetneq (f_i) \subset \mathfrak{p} \subsetneq \mathfrak{m},$$

for some maximal ideal $\mathfrak{m}$. Hence, $(f_i) = \mathfrak{p}$, by Theorem 23.5.8. □

(Try to do this by hand! It is a nontrivial task. And of course this is just for $n = 2$.)

23.6. **Structure theorem for modules over a PID.** Let A be a PID. Our goal for the rest of the semester is to prove:

Theorem 23.6.1. *Let M be a finitely generated A-module. Then M can be written as a direct sum of modules of the following two types:*

- $M = A$;
- $M = A/\mathfrak{m}^n$ *for a maximal ideal* $\mathfrak{m} \subset A$ *and* $n \neq 0$.

That is, M is a (finitely generated) free module direct summed with a finite direct sum of "cyclic" modules. (The wording is meant to suggest the case of $\mathbb{Z}$.)

Let us see what this theorem says in some familiar cases.

23.6.2. Take $A = \mathbb{Z}$. Then we obtain the (familiar) structure theorem for finitely-geneated abelian groups: any such group is a direct sum of factors of the following two types:

- $\mathbb{Z}$,
- $\mathbb{Z}/p^n\mathbb{Z}$, where p is a prime number.

23.6.3. Take $A = k[t]$. Let us take M to be such that it is finite-dimensional as a k-vector space. Then we can think of M as a finite-dimensional vector space V, acted on by a linear operator T.

From Theorem 23.6.1 we obtain that V decomposes as a direct sum of T-invariant subspaces, each of which is isomorphic to some

$$k[t]/(p(t))^n,$$

where $p(t) \in k[t]$ is irreducible, and where T acts by multiplication by t.

Note that when $n = 1$, such a direct summand is a field extension $k' \supset k$, where T acts as multiplication by some element $x' \in k' - k$.

Assume for the moment that k is algebraically closed, so $p(t) = (t - \lambda)$ for $\lambda \in k$. Note that $k[t]/(t - \lambda)^n$ identifies with the Jordan block of length n and eigenvalue λ. To see this, write the multiplication by t in the basis

$$1, (t - \lambda), (t - \lambda)^2, \ldots, (t - \lambda)^{n-1}.$$

23.7. **Discrete valuation rings.**

23.7.1. A local PID, which is not a field, is called a discrete valuation ring (DVR). The reason for the name, as we will see, is that such a thing admits a discrete valuation (i.e., a measure of size taking values in $\mathbb{N}$, like the p-adic valuation).

Here is how one generally constructs a DVR:

Lemma 23.7.2. *A localization of a PID at a nonzero prime is a DVR.*

Proof. It suffices to show that a localization of a PID is again a PID. However, this follows from the description of ideals in A_S in terms of the ideals of A — see Proposition 20.2.7. □

23.7.3. Let A be a DVR and let $\mathfrak{m}$ denote its maximal ideal. We have $\mathfrak{m} = (\pi)$ for some prime element $\pi \in A$. Such a π is called a *uniformizer* (or *uniformizing element*) of A. Evidently, if π_1 and π_2 are two uniformizers, then

$$\pi_1 = \pi_2 \cdot u,$$

where $u \in R$ is invertible (consider the ideals generated by them).

23.7.4. Since A is local, π is the *only* irreducible element in A (up to multiplication by a unit). Decomposition into irreducibles (see Proposition 19.2.6 and Lemma 19.3.6) implies:

Lemma 23.7.5. *Any element in A can be uniquely written as $\pi^n \cdot u$, where u is invertible.*

Corollary 23.7.6. *The nonzero ideals of A are all of the form $\mathfrak{m}^n = (\pi^n)$.*

23.7.7. Hence we have a well-defined function

$$v : A - \{0\} \to \mathbb{N}, \quad v(\pi^n \cdot u) := n.$$

It is easy to see that $v(-)$ does not depend on the choice of the uniformizer π — this because $v(a) = \min\{n | a \in \mathfrak{m}^n\}$. Indeed, we have:

Lemma 23.7.8. $v(a) \geq n \Leftrightarrow a \in \mathfrak{m}^n$.

23.7.9. Let K denote the faction field of A. Note that any element of K can be uniquely written as

$$\pi^n \cdot u,$$

where $n \in \mathbb{Z}$ and u is an invertible element of A.

Hence we can extend v to a function:

$$v : K - \{0\} \to \mathbb{Z}, \quad v(\pi^n \cdot u) := n.$$

For notational convenience, taking $v(0) := +\infty$ is often convenient, but we won't do so here.

Proposition 23.7.10. *v satisfies:*

(1) $v(x \cdot y) = v(x) + v(y)$.
(2) *For $x + y \neq 0$, we have $v(x + y) \geq \min(v(x), v(y))$ and the inequality is an equality if $v(x) \neq v(y)$.*

A v satisfying the above is called a *discrete valuation* — hence, as mentioned above, the terminology "DVR". The prototypical example of such a thing is the "order of vanishing at 0", taking a power series

$$0 \neq f(X) =: \sum_{n=0}^{\infty} a_n X^n$$

to the smallest $n =: \mathrm{ord}_0 f$ such that $a_n \neq 0$. That is, were the power series convergent in some small neighborhood of zero, it would define a function of $X \in \mathbb{C}$ (say) for $|X|$ sufficiently small. Then $\mathrm{ord}_0 f$ would be the order of vanishing of f:

$$f(0) = 0, f'(0) = 0, \ldots, f^{(n-1)}(0) = 0, \text{ but } f^{(n)}(0) \neq 0.$$

If f were a polynomial, then

$$f(X) = X^{\mathrm{ord}_0 f} g(X)$$

with $g(0) \neq 0$.

The extension to the fraction field corresponds to extending the "order of vanishing" to power series that have poles at 0:

$$\mathrm{ord}_0 \left(\sum_{n=-n_0}^{\infty} a_n X^n \right) := n_0 \quad (a_{n_0} \neq 0).$$

The first claim of the proposition corresponds to the fact that if $f(X) = X^m \tilde{f}(X)$ with $\tilde{f}(0) \neq 0$ and $g(X) = X^n \tilde{g}(X)$ with $\tilde{g}(0) \neq 0$, then

$$(fg)(X) = X^{m+n}(\tilde{f}\tilde{g})(X),$$

and $(\tilde{f}\tilde{g})(0) = \tilde{f}(0)\tilde{g}(0) \neq 0$. The second corresponds to the fact that if $m \leq n$, then

$$(f + g)(X) = X^m(\tilde{f}(X) + X^{n-m}\tilde{g}(X)).$$

Moreover if $m < n$, then the second summand vanishes at 0, so that the order is precisely m. In fact the ring of formal power series is itself a DVR, and we will see this in a moment. But first:

Week 12, Problem 3. *Prove Proposition 23.7.10.*

23.7.11. The following material was not presented in class:

Theorem 23.7.12. *Let A be a local Noetherian domain with maximal ideal $\mathfrak{m}$. The following conditions are equivalent:*

(a) *A is a DVR;*

(b) $\dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = 1$*;*

(c) *The ideal $\mathfrak{m}$ is principal (i.e., of the form (f) for some $f \in A$);*

(d) *There exists an element $f \in \mathfrak{m}$ such that any $a \in A$ can be written as $f^n \cdot u$ with u invertible.*

As promised, here is our example again:

Corollary 23.7.13. *The following ring is a DVR: $A = k[[t]]$.*

Proof. The maximal ideal in A is $t \cdot k[[t]]$ and it is evidently unigenerated (here we are using the fact that power series with nonzero constant term are invertible — this follows from the formula for the geometric series). □

23.7.14. The proof of Theorem 23.7.12 uses the following result, of huge importance in commutative algebra:

Theorem 23.7.15 (Nakayama's Lemma)**.** *Let A be a local ring with maximal ideal $\mathfrak{m}$, and M a finitely generated A-module. Then $M/\mathfrak{m} \cdot M = 0$ if and only if $M = 0$.*

Proof (due to Jean-Pierre Serre). Assume first that $0 \neq M$ is unigenerated. In this case $M \simeq A/I$ for some ideal $I \subset A$. Since A is local, we have $I \subset \mathfrak{m}$. Hence $M/\mathfrak{m} \cdot M \simeq \overline{A}/\overline{\mathfrak{m}} \simeq A/\mathfrak{m}$, where $\overline{A} = A/I$ and $\overline{\mathfrak{m}} = \mathfrak{m}/I$. In this case the assertion is manifest.

For a general finitely-generated $0 \neq M$, there exists a finite filtration

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n = M.$$

where each M_i/M_{i-1} is uni-generated (namely, just add a generator at each step). Without loss of generality $M_n/M_{n-1} \neq 0$, hence

$$(M_n/M_{n-1})/\mathfrak{m} \cdot (M_n/M_{n-1}) \neq 0.$$

However, $(M_n/M_{n-1})/\mathfrak{m} \cdot (M_n/M_{n-1})$ is a quotient of $M_n/\mathfrak{m} \cdot M_n$, and hence the latter isn't zero either.

□

Corollary 23.7.16. *In a local Noetherian ring A, if $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ then $\mathfrak{m}^n = 0$.*

Proof. Apply Theorem 23.7.15 to $M = \mathfrak{m}^n$. □

Corollary 23.7.17. *Let A be a local ring with maximal ideal $\mathfrak{m}$, and M a finitely generated A-module. Let $T : M' \to M''$ be a map of A-modules such that the induced map $M'/\mathfrak{m} \cdot M' \to M''/\mathfrak{m} \cdot M''$ is surjective. Then T is surjective.*

Proof. Apply Theorem 23.7.15 to $M := \operatorname{coker}(M' \to M'')$. □

(Do you see why with Nakayama we can only prove surjectivity and not injectivity?)

The beautiful thing about Nakayama's lemma is that it reduces checking things about maps or modules over a local ring (which may be horribly complicated) to a question of linear algebra: after all, $M/\mathfrak{m} \cdot M$ is a vector space over the "residue field" $A/\mathfrak{m}$!

23.7.18. *Proof of Theorem 23.7.12.* The implication (a) $\Rightarrow$ (c) is tautological.

Notice that by Corollary 23.7.16, $\mathfrak{m}^2 \neq \mathfrak{m}$ for any local Noetherian ring. In particular, $\dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) \geq 1$.

For the implication (c) $\Rightarrow$ (b), we note that if f is a generator of $\mathfrak{m}$, then the $A/\mathfrak{m}$-vector space $\mathfrak{m}/\mathfrak{m}^2$ is spanned by the image of f. Hence, $\dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) \leq 1$ (and hence it is equal to 1).

Let us prove (b) $\Rightarrow$ (c). Let f be an element of $\mathfrak{m} - \mathfrak{m}^2$. By assumption, its image in $\mathfrak{m}/\mathfrak{m}^2$ spans $\mathfrak{m}/\mathfrak{m}^2$. Consider the map of A-modules,

$$A \to \mathfrak{m}, \quad 1 \mapsto f.$$

This map is surjective by Corollary 23.7.17. Hence f generates $\mathfrak{m}$.

Let us prove that (c) $\Rightarrow$ (d). Let f be a generator of $\mathfrak{m}$. In particular, f^n is a generator of $\mathfrak{m}^n$. First, we claim that $\bigcap_n \mathfrak{m}^n = 0$. Indeed,

$$I := \bigcap_n \mathfrak{m}^n$$

is the set of elements divisible by any power of f. Now, it is clear that $f : I \to I$ is a surjection, and so the fact that $I = 0$ follows from Theorem 23.7.15.

For an element $a \in A$, let n be the maximal integer such that a is divisible by f^n. Write $a = f^n \cdot b$. We claim that b is a unit. Indeed, $f \nmid b$ means that $b \notin \mathfrak{m}$.

Finally, let us prove that (d) $\Rightarrow$ (a). Let $I \subset A$ be a proper nonzero ideal. Take $0 \neq a \in I$ and write it as $a =: f^n \cdot u$ with u invertible. Since u is invertible, we obtain that $f^n \in I$. Now let n_0 be the minimal integer such that $f^{n_0} \in I$ (one exists since $n_0 \leq n$). We claim that $(f^{n_0}) = I$. Indeed, for any $b \in I$, writing $b =: f^m \cdot u$, $m \geq n_0$, so b is divisible by f^{n_0}.

□

24. Thursday, April 25

24.1. **Torsion.**

24.1.1. Let A be a domain and M an A-module.

Definition 24.1.2. *An element $m \in M$ is said to be* torsion *if there exists $0 \neq a \in A$ such that $a \cdot m = 0$.*

Let $M^{\mathrm{tors}} \subset M$ be the subset of torsion elements.

Lemma 24.1.3. *M^{tors} is an A-submodule.*

Proof. Do it yourself. □

Definition 24.1.4. *We shall say that M is* torsion *(resp.,* torsion-free*) if $M^{\mathrm{tors}} = M$ (resp., $M^{\mathrm{tors}} = 0$).*

Lemma 24.1.5. *The quotient module M/M^{tors} is torsion-free.*

Proof. Do it yourself. □

24.1.6. We have the following useful characterization of torsion (resp., torsion-free) modules.

Proposition 24.1.7. *Let K denote the field of fractions of A.*
(a) *A module M is torsion if and only if $K \underset{A}{\otimes} M = 0$.*
(b) *A module M is torsion-free if and only if the canonical map $M \to K \underset{A}{\otimes} M$ is injective.*

Week 12, Problem 4. *Prove Proposition 24.1.7.*

In addition, we have:

Proposition 24.1.8. *Let M be an A-module. Then the following conditions are equivalent:*
(a) *M is torsion.*
(b) $(0) \notin \mathrm{supp}(M)$.
(c) $\mathrm{supp}(M) \neq \mathrm{Spec}(A)$.

Proof. The equivalence of (a) and (b) follows from Proposition 24.1.7 (after all, localizing at (0) is the same thing as tensoring with the fraction field). Clearly, (b) implies (c). We will prove that (c) implies (b) under the assumption that M is finitely generated.

Week 12, Problem 5. *Generalize the argument below to the case when M is arbitrary.*

If M is finitely generated, set $I := \mathrm{Ann}(M)$. By Theorem 22.2.4, $\mathrm{supp}(M) = V(I)$. Hence, $V(I) \neq \mathrm{Spec}(A)$. Since A is a domain, this means that $I \neq 0$. This means that $(0) \notin V(I)$.

□

24.2. **Theorem 23.6.1 for torsion modules.** Our current goal is to prove the following particular case of 23.6.1:

Theorem 24.2.1. *Let A be a PID and let M be a finitely generated A-module. Then M can be written as a direct sum of modules of the form $M = A/\mathfrak{m}^n$ for a maximal ideal $\mathfrak{m} \subset A$ and $n \neq 0$.*

24.2.2. We have the following result:

Proposition 24.2.3. *Let A be Noetherian, and let M be an A-module whose support is a union of closed points. Then M splits as a direct sum*

$$M \simeq \bigoplus_i M_i,$$

indexed by the set of maximal ideals $\mathfrak{m}_i$ in the support of M, such that $\mathrm{supp}(M_i) = \{\mathfrak{m}_i\}$. *Moreover, for every i, the canonical map $M \to M_{\mathfrak{m}_i}$ factors as*

$$M \to M_i \to M_{\mathfrak{m}_i},$$

where the second arrow is an isomorphism.

We will prove this proposition assuming that M is finitely generated.

Week 12, Problem 6. *Generalize the proof below to the case when M is arbitrary.*

Proof. Let $I := \mathrm{Ann}(M)$, so we can regard M as a module over $\overline{A} := A/I$. The assumption implies that any prime in $\overline{A}$ is maximal. Hence $\overline{A}$ is an Artinian ring. In this case, the assertion follows from Proposition 23.4.4.

□

Corollary 24.2.4. *Let A be a domain of Krull dimension 1, and let M be a torsion A-module. Then M splits as a direct sum*

$$M \simeq \bigoplus_i M_i,$$

indexed by the set of maximal ideals $\mathfrak{m}_i$ of A, such that $\mathrm{supp}(M_i) = \{\mathfrak{m}_i\}$. Moreover, for every i, the canonical map $M \to M_{\mathfrak{m}_i}$ factors as

$$M \to M_i \to M_{\mathfrak{m}_i},$$

where the second arrow is an isomorphism.

24.2.5. Note that if A is a ring and $\mathfrak{m}$ is a maximal ideal, then the module $A/\mathfrak{m}^n$ has the property that the canonical map

$$A/\mathfrak{m}^n \to (A/\mathfrak{m}^n)_{\mathfrak{m}}$$

is an isomorphism (indeed, the ring $A/\mathfrak{m}^n$ is local). Hence,

$$A/\mathfrak{m}^n \simeq A_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}}^n,$$

where $\mathfrak{m}_{\mathfrak{m}} \subset A_{\mathfrak{m}}$ is the unique maximal ideal.

Hence, using Corollary 24.2.4, we obtain that the assertion of Theorem 24.2.1 reduces to the case when A is a DVR (replace A by $A_{\mathfrak{m}}$, where $\mathfrak{m}$ is a maximal ideal in A).

24.2.6. *Proof of Theorem 24.2.1 over a DVR.* Note that by Theorem 22.4.2, finitely generated torsion modules over A have finite length. By induction, we can assume that the desired decomposition exists for modules of length smaller than the length of M (check the base of the induction!).

Step 1. Let π be a uniformizer of A. Let n be the smallest integer such that π^n annihilates M. Let $m \in M$ be an element such that $\pi^{n-1} \cdot m \neq 0$. Consider the map

$$A \to M, \quad 1 \to m.$$

Its kernel is an ideal that contains (π^n), but does not contain (π^{n-1}). Since every ideal in A is of the form (π^k) for some k, we obtain that the above kernel equals (π^n).

Consider the resulting short exact sequence

$$0 \to A/\pi^n \cdot A \to M \to M' \to 0. \tag{24.1}$$

(That is, $M' := M/A \cdot m$.)

By the induction hypothesis, M' splits as a direct sum of the desired form, since it has strictly smaller length. Hence, it remains to show that the short exact sequence (24.1) splits.

Step 2. Let

$$0 \to M'' \to M \to M' \to 0 \tag{24.2}$$

be a short exact sequence of modules over an arbitrary ring. Let $M' := M'_1 \oplus M'_2$. Let M_1 and M_2 denote the respective preimages of M'_1 and M'_2 in M.

We obtain the short exact sequences:

$$0 \to M'' \to M_1 \to M'_1 \to 0 \tag{24.3}$$

and

$$0 \to M'' \to M_2 \to M'_2 \to 0. \tag{24.4}$$

Lemma 24.2.7. *The datum of a splitting of the short exact sequence* (24.2) *is equivalent to the datum of a splitting of each of the short exact sequences* (24.3) *and* (24.4) *separately.*

Proof. Do it yourself. □

Hence, it remains to show that a short exact sequence

$$0 \to A/\pi^n \cdot A \xrightarrow{i} M \xrightarrow{p} A/(\pi^k) \to 0 \tag{24.5}$$

splits, where M has the property that it is annihilated by π^n (in particular, $k \leq n$).

Step 3. To split (24.5) is equivalent to finding an element $m \in M$ such that

- $p(m) = \overline{1} \in A/\pi^k \cdot A$;
- $\pi^k \cdot m = 0$.

I.e., we have to show that such an element exists. Let $m' \in M$ be *any* element such that $p(m') = \overline{1}$. We need to show that there exists an element $\overline{b} \in A/\pi^n$ such that $m := m' - i(\overline{b})$ satisfies $\pi^k \cdot m = 0$. We rewrite this condition as

$$\pi^k \cdot m' = i(\pi^k \cdot \overline{b}).$$

Note that $p(\pi^k \cdot m') = \pi^k \cdot \overline{1} = 0$. Hence,

$$\pi^k \cdot m' = i(\overline{a})$$

for some $\overline{a} \in A/\pi^n$.

Hence, we need to show that there exists $\overline{b} \in A/\pi^n$ such that $\pi^k \cdot \overline{b} = \overline{a}$, i.e., that $\overline{a}$ lies in the image of the multiplication by π^k.

Step 4. We note that

$$i(\pi^{n-k} \cdot \overline{a}) = \pi^n \cdot m' = 0.$$

Since i is injective, we obtain that $\pi^{n-k} \cdot \overline{a} = 0$. Now, the required assertion follows from the next lemma:

Lemma 24.2.8. *If A is a DVR with uniformizer π, for $k \leq n$, the image of the multiplication by π^k on $A/\pi^n \cdot A$ equals the kernel of the multiplication by π^{n-k}.*

Proof. Do it yourself. □

Q.E.D. Theorem 24.2.1. □

24.3. **Theorem 23.6.1 for torsion-free modules.** The goal of this subsection is to pove another particular case of Theorem 23.6.1:

Theorem 24.3.1. *Let A be a PID, and let M be a finitely generated torsion-free module. Then $M \simeq A^{\oplus n}$.*

24.3.2. Let us first see how Theorems 24.3.1 and 24.2.1 combined yield Theorem 23.6.1:

Proof of Theorem 23.6.1. Consider the short exact sequence

$$0 \to M^{\mathrm{tors}} \to M \to M/M^{\mathrm{tors}} \to 0, \tag{24.6}$$

where M/M^{tors} is torsion-free by Lemma 24.1.5.

By Theorems 24.2.1, the quotient M/M^{tors} is isomorphic to $A^{\oplus n}$ for some n. But then it is a free module, and any surjection onto a free module splits (just choose preimages of a basis). Hence the short exact sequence (24.6) splits — i.e.,

$$M \simeq M^{\mathrm{tors}} \oplus A^{\oplus n}.$$

Now, the assertion of Theorem 23.6.1 follows from that of Theorem 24.2.1.

□

24.3.3. We will deduce Theorem 24.3.1 from the following result:

Theorem 24.3.4. *Let A be a PID with fraction field K. Let M be a finitely generated A-submodule of K. Then $M = f \cdot A$ for some $f \in K$.*

(It turns out such modules correspond to line bundles over $\mathrm{Spec}(A)$, like the Mobius band over S^1, and the point is that over such rings all line bundles are trivial — i.e., they look like $\mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n$ (just a straight line over each point, with no twisting as in the Mobius band).)

Remark 24.3.5. Submodules L as in Theorem 24.3.4 are called *fractional ideals*.

For example, we might consider $\frac{1}{2}\mathbb{Z} + \frac{1}{3}\mathbb{Z} + \frac{1}{5}\mathbb{Z} \subset \mathbb{Q}$, but this is just $\frac{1}{30}\mathbb{Z}$.

Corollary 24.3.6. *Let A be a PID with fraction field K. Let M be a finitely generated A-submodule of K. Then $M \cong A$ as A-modules.*

Let us see how Theorem 24.3.4 implies Theorem 24.3.1:

Proof of Theorem 24.3.1. Consider the embedding of A-modules

$$M \hookrightarrow K \underset{A}{\otimes} M$$

(see Proposition 24.1.7).

Consider $K \underset{A}{\otimes} M$ as a K-vector space; denote it by V. Choose a filtration

$$0 = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_{n-1} \subsetneq V_n = V,$$

where $\dim_K(V_i/V_{i-1}) = 1$. Write

$$M_i := M \cap V_i \subset V.$$

We obtain a filtration (potentially with repeats!)

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{n-1} \subseteq M_n = M,$$

and embeddings

$$M_i/M_{i-1} \hookrightarrow V_i/V_{i-1} \simeq K.$$

Since A is Noetherian, the module M_i is finitely generated, and hence so is M_i/M_{i-1}. By Corollary 24.3.6, we obtain that each M_i/M_{i-1} is either zero or isomorphic to A.

Consider the short exact sequence

$$0 \to M_{n-1} \to M_n \to M_n/M_{n-1} \to 0.$$

If $M_n/M_{n-1} \simeq A$, the above short exact sequence splits. I.e.,

$$M = M_n \simeq M_{n-1} \oplus A.$$

Otherwise $M_{n-1} = M_n$ tautologically.

Iterating, the theorem follows.

□

24.3.7. Finally, let us prove Theorem 24.3.4. We will use the following assertion:

Lemma 24.3.8. *Let A be a domain with fraction field K, and let M be a finitely generated A-submodule in K. Then there exists an element $g \in A$ such that multiplication by g maps M isomorphically onto an ideal in A.*

As with the example of $\frac{1}{30}\mathbb{Z}$, this will amount to clearing denominators.

Proof. Let $m_1, \ldots, m_n$ be generators of M. Write

$$m_i =: \frac{a_i}{b_i}.$$

Take

$$g := \prod_{i=1}^{n} b_i.$$

□

Proof of Theorem 24.3.4. By Lemma 24.3.8, we can find an element g such that multiplication by g isomorphs M onto an ideal $I \subset A$. Since A is a PID, we have $I =: (h) = A \cdot h$ for some $h \in A$. The sought-for element f is $f := \frac{h}{g}$ (i.e., $M = \frac{h}{g} \cdot A$). □

Remark 24.3.9. For an alternative proof of Theorem 24.3.4 and generalizations, see the mini-project on Dedekind domains.

24.4. **Structure of torsion modules over a PID.** In this subsection we let M be a finitely generated torsion module over a PID A.

Write

$$M \simeq \bigoplus_i M_i,$$

where $\mathrm{supp}(M_i) = \{\mathfrak{m}_i\}$.

Note that M is of finite length (and hence so are the M_i), by Theorem 22.4.2. Set

$$n_i := \lg(M_i).$$

Consider the ideals

$$\mathrm{ch}(M) := \prod_i \mathfrak{m}_i^{n_i}$$

and

$$\min(M) := \mathrm{Ann}(M).$$

Week 12, Problem 7. *Let $A = k[t]$, and let us think of M as a vector space V over k, equipped with en endomorphism T. Suppose this vector space is finite-dimensional. Show that* $\mathrm{ch}(M)$ *(resp.,* $\min(M)$*) is generated by the characteristic (resp., minimial) polynomial of T on V.*

Week 12, Problem 8. *Show that* $\mathrm{ch}(M) \subset \min(M)$.

Week 12, Problem 9. *Show that M is* completely reducible *if and only if* $\min(M) = \prod_i \mathfrak{m}_i$.

Week 12, Problem 10. *Show that the following conditions are equivalent:*

(a) $\mathrm{ch}(M) = \min(M)$.

(b) *M is uni-generated.*

(c) *Every M_i is uni-generated.*

(d) *The map $A/\operatorname{Ann}(M) \to \operatorname{End}_A(M)$, given by the action of A on M, is an isomorphism.*