Algebra II Notes: A Whole Bunch of Algebra

Transcribed by William Jones; Taught by Alexander Borisov

Contents

Chapter 1

Topics in Group Theory

1.1 1/26/22: Introduction to Group Actions

Let G be a group and $\Omega \neq \varnothing$. A map $G \times \Omega \to \Omega$ by the rule $(g, \alpha) \mapsto g \bullet \alpha$ is a **left group action** if:

1. $1 \bullet \alpha = \alpha$ for all $\alpha \in \Omega$, and
2. $g \bullet (h \bullet \alpha) = (gh) \bullet \alpha$ for all $g, h \in G$, and $\alpha \in \Omega$.

If such an action exists, we say that, equivalently, G **acts on** Ω **by** $\bullet$, G **acts on** Ω, or Ω is a G**-set**. In general, we call $\omega \in \Omega$ a **point**.

We can immediately construct many general examples. In all of the following, G is a group, and Ω is a (unless otherwise specified) arbitrary set.

- **The trivial action**. We can define:

$$g \bullet \alpha = \alpha$$

  for all $g \in G$. This is easily a group action.

- **The regular action**. If $\Omega = G$, then we can define:

$$g \bullet \alpha = g\alpha$$

  This is a group action because G is a group.

- **The natural action of** S_n **on** $[n]$. Let $n \geqslant 1$, and $\Omega = [n]$. Then S_n acts on Ω by:

$$\sigma \bullet i = \sigma(i)$$

  We verify the second requirement for a group action:

$$\begin{aligned} \sigma \bullet (\tau \bullet i) &= \sigma \bullet (\tau(i)) \\ &= \sigma(\tau(i)) \\ &= (\sigma \circ \tau)(i) \\ &= \sigma\tau \bullet i \end{aligned}$$

- **The translation action**. Let $H \leq G$, and $\Omega = G$. Then define:

$$h \bullet g = hg$$

  for all $h \in H$, and $g \in G$.

- **The conjugation action**. Let $\Omega = G$, and define:

$$g \bullet \alpha = g\alpha g^{-1}$$

  In this case, notice that we need the inverse to be on the right-hand side; the proof does not work if g is conjugated in the other way. On the other hand, if we consider an analogously defined **right group action**, then we would have $\alpha \circ g = g^{-1}\alpha g$.

- **The conjugation action on subgroups**. Let $\Omega = \mathcal{S}$, the set of all subgroups of G. Then define:

$$g \bullet H = gHg^{-1}$$

  for all $H \leq G$.

What can we say about group actions? Quite a lot, but we will present some elementary results.

Lemma 1. *Let a group G act on Ω. For $g \in G$, define $\sigma_g : \Omega \to \Omega$ by $\sigma_g(\alpha) = g \bullet \alpha$, for all $\alpha \in \Omega$. Then σ_g is a bijection on Ω.*

Proof. Observe that σ_g has inverse $\sigma_{g^{-1}}$. □

If G acts on Ω, this gives that $\sigma_g \in \mathrm{Sym}(\Omega)$, and we obtain a group homomorphism $G \to \mathrm{Sym}(\Omega)$ by $g \mapsto \sigma_g$. Notice that we can retrieve Cayley's Theorem from letting $\bullet$ be the regular action.

If we let Σ be that homomorphism, we say that $\ker(\Sigma)$ is the **kernel of the action**. If the action has trivial kernel, then we say that G acts **faithfully** on Ω.

The next construction is quite general, and powerful for it. Let a group G act on Ω, and $\alpha \in \Omega$. The set:

$$\mathrm{Stab}_G(\alpha) = \{g \in G : g \bullet \alpha = \alpha\}$$

is called the **stabilizer of α in G**.

Two concrete examples of stabilizers are things we have seen before, albeit briefly. If we let $\bullet$ be conjugation and $a \in G$, then:

$$\mathrm{Stab}_G(a) = \{g \in G : ga = ag\} = C_G(a),$$

the **centralizer of a in G**. On the other hand, if we let $\bullet$ be conjugation *of subgroups*, and $H \leq G$, then:

$$\mathrm{Stab}_G(H) = \{g \in G : gH = Hg\} = N_G(H),$$

the **normalizer of $H \leq G$**.

Notice that both of these are subgroups of G. Indeed:

Lemma 2. $\mathrm{Stab}_G(a)$ *is a subgroup of* G

Proof. Clearly $e \in \mathrm{Stab}_G(a)$. Suppose $g, h \in stab_G(a)$. Then $g \bullet \alpha = \alpha$ and $h \bullet \alpha = \alpha$. Then:

$$(gh) \bullet \alpha = g \bullet (h \bullet \alpha) = g \bullet \alpha = \alpha$$

so $gh \in \mathrm{Stab}_G(a)$. Last, if $g \bullet \alpha = \alpha$, then:

$$g^{-1} \bullet \alpha = g^{-1} \bullet (g \bullet \alpha) = e \bullet \alpha = \alpha$$

Thus $\mathrm{Stab}_G(a) \leq G$. □

It is natural to consider where the group action sends points of Ω. We define an **orbit** of G on Ω containing α to be:

$$O_\Omega(\alpha) :=: O(\alpha) :=: G \bullet \alpha := \{g \bullet \alpha : g \in G\}$$

If G has only one orbit on Ω, we say that G acts **transitively** on Ω. As it turns out, $O(\alpha)$ is *the* orbit containing α, as we shall soon see. But first, a concrete example that shows this generalizes what we have seen. If G acts on itself by conjugation and $a \in G$, then:

$$O_G(a) = \{gag^{-1} : g \in G\}$$

the **conjugacy class** of G containing a. More evidence that orbits partition Ω! Indeed, on Ω define $\alpha \sim \beta$ if there is $g \in G$ so that $\beta = g \bullet \alpha$. One can verify this is an equivalence relation, and the equivalence classes of $\sim$ are nothing but the distinct orbits of G on Ω. This also suggests we can extract information about the size of $O(\alpha)$.

This is not surprising; after all, no matter what shape Ω takes, the action structure is one-to-one with G's group structure, so quantitative information about the orbits of Ω under G's action are controlled by quantitative information about G. The size of an orbit should be controlled by how many elements of g can act on α without returning α; i.e., how many left cosets of $\mathrm{Stab}_G(\alpha)$ are in G. Fortunately, this is the case!

Theorem 1 (Orbit-Stabilizer Lemma)**.** *Let* G *act on* Ω*, and* $\alpha \in \Omega$*. Then:*

$$|O_\Omega(\alpha)| = (G : \mathrm{Stab}_G(\alpha))$$

where $(G : H)$ *is the index of* H *in* G*.*

Proof. Let $H = \mathrm{Stab}_G(\alpha)$. We construct a bijection:

$$b : \{gH : g \in G\} \to O_\Omega(\alpha)$$

by the rule $gH \mapsto g \circ \alpha$. First, we check that b is well-defined. Suppose that $aH = bH$. Then $b^{-1}a \in H$, so $b^{-1}a \bullet \alpha = \alpha$. Hence $b \bullet (b^{-1}a \bullet \alpha) = b \bullet \alpha$, which is what we wanted.

Now we show bijectivity; if $a \bullet \alpha = b \bullet \alpha$, then $b^{-1}a \in H$, so $aH = bH$. If $\omega \in O_\Omega(\alpha)$, then there is some $g \in G$ so that $g \bullet \alpha = \omega$, thus $gH \in b^{-1}(\omega)$. □

This gives information on *any* group action, which is quite helpful. In particular, we can get a nice corollary for finite considerations:

Corollary 1. *If finite G is acting on finite Ω, and $\alpha \in \Omega$, then:*

$$|O(\alpha)| = \frac{|G|}{|\mathrm{Stab}_G(\alpha)|}$$

Which gives some nice results in finite group theory; in particular, if G is a group, $a \in G$, and $H \leq G$, we get information about the conjugacy classes of a and H:

$$|\{gag^{-1} : g \in G\}| = \frac{|G|}{|C_G(a)|}, \text{ and } |\{gHg^{-1} : g \in G\}| = \frac{|G|}{|N_G(H)|}$$

1.2 1/28/22: More On Group Orbits, and Elementary Sylow Theory

This section involves an application of group orbits to group structure; i.e., understanding how results in group action theory apply to a group acting on itself.

First, define the **fixed-point set** of Ω under G's action to be:

$$\mathrm{Fix}_\Omega(G) = \{\alpha \in \Omega : O_\Omega(\alpha) = \alpha\} = \{\alpha \in \Omega : g \bullet \alpha = \alpha, \forall g \in G\}$$

Then by the fact that the $O(\alpha)$ partition Ω:

Theorem 2 (The General Class Equation)**.** *Suppose G acts on Ω, and $\{O_i\}_{i\in[k]}$ is the collection of distinct orbits of elements of Ω of size at least 2. Then:*

$$\Omega = \mathrm{Fix}_\Omega(G) \sqcup \bigsqcup_{i\in[k]} O_i$$

If G is finite, $\Omega = G$, the action is conjugation, and $a_i \in O_i$ as in Theorem 2, we obtain by the Orbit-Stabilizer lemma the more-famous **class equation**:

$$|G| = |Z(G)| + \sum_{i\in[k]} \frac{|G|}{|C_G(a_i)|}$$

where $Z(G)$ is the **center** of G.

This is a useful tool for questions of divisibility, as it allows for induction. In particular, we will be making use of it in showing:

Theorem 3 (Cauchy's Theorem)**.** *Let G be finite and p be a prime so that p divides $|G|$. Then G has an element of order p.*

Proof. We prove this by induction on $|G|$. There are several cases to consider.

Case 1: G is abelian.

If G is abelian, then $G = Z(G)$. Pick $g \neq e \in G$, and write $\mathrm{ord}_G(g) = m > 1$. If $m = p$, we are done, so assume not.

Case 1.1: p divides m.

If $p|m$, then let $a = g^{m/p}$. Since $m \neq p$, we know that $a \neq e$. Moreover, as $a^p = (g^{m/p})^p = g^m = e$, it follows that $\mathrm{ord}_G(a)$ divides p. Since $\mathrm{ord}_G(a) > 1$ and p is prime, it has to be that $\mathrm{ord}_G(a) = p$, so we are done.

Case 1.2: p does not divide m.

If p does not divide m, then consider $G/\langle g\rangle$ (notice this is where we use that G is abelian). By the case and the fact that $|G/\langle g\rangle| = |G|/m$, it holds that p divides $|G/\langle g\rangle|$, so by induction $|G/\langle g\rangle|$ has an element $[x]$ so that $\mathrm{ord}_{G/\langle g\rangle}([x]) = p$. Then $x^p \in \langle g\rangle$, so $x^p = g^k$ for some $k \in \mathbb{Z}$. Since $\mathrm{ord}_G(g^k)$ divides $\mathrm{ord}_G(g) = m$, it holds that $x^{pm} = e$.

Notice that since $x \mapsto [x]$ is a group homomorphism, then $\mathrm{ord}_{G/\langle g\rangle}([x])$ divides $\mathrm{ord}_G(x)$; i.e., p divides $\mathrm{ord}_G(x)$. If it is the case that $x^m = e$, then $\mathrm{ord}(x)|m$, which would imply that $p|m$, which is impossible by the case. Thus $x^m \neq e$, so by the conclusion

of the previous paragraph, p divides $\mathrm{ord}(x)$, and we can proceed as in Case 1.1 to find $\tilde{x} \in G$ of order p.

Case 2: G is not abelian. In this case, we make use of the class equation:

$$|G| = |Z(G)| + \sum_{i \in [k]} \frac{|G|}{|C_G(a_i)|}$$

The premise is the same as stating that the class equation is nontrivial; i.e., the right-hand summation is nonzero.

Case 2.1: p does not divide $|G|/|C_G(a_j)|$ for some j.

It follows that all powers of p (and possibly more) are factored out of $|G|$ by $|C_G(a_j)|$; i.e., p divides $|C_G(a_j)|$. Since this is a strictly smaller order than $|G|$, induction gives an element of order p in a subgroup of G, thus in G.

Case 2.2: p divides $|G|/|C_G(a_i)|$ for all i.

Since $|Z(G)| = |G| - \sum_{i \in [k]} \frac{|G|}{|C_G(a_i)|}$, it holds that p divides $|Z(G)|$, and we can proceed either with induction, or the reasoning of Case 1.

□

We say a group G is a p**-group** if $\mathrm{ord}(g) = p^{k_g}$ for all $g \in G$.

Corollary 2. *If G is a finite p-group, p prime, then $|G| = p^k$ for some $n \geqslant 0$.*

Indeed, if $|G|$ had another prime factor, then by Cauchy's Theorem, G would have an element of order q, hence would not be a p-group.

We can also get some information directly from the class equation:

Corollary 3. *If G is a nontrivial p-group, p prime, then $|Z(G)| > 1$.*

Indeed, this is just Case 2.2 of Cauchy's Theorem.

We can also get a sibling result for group orbits; in the following, we are assuming that G is finite.

Theorem 4 (Fixed-Point Congruence of p-Groups)**.** *Let G be a p-group, p prime, acting on finite Ω. Then:*

$$|\mathrm{Fix}_\Omega(G)| \equiv_p |\Omega|$$

Proof. Using the general class equation, $\Omega = \mathrm{Fix}_\Omega(G) \sqcup \bigsqcup_{i \in [k]} O_i$, the Orbit-Stabilizer lemma gives:

$$|\Omega| = |\mathrm{Fix}_\Omega(G)| + \sum_{i \in [k]} \frac{|G|}{|\mathrm{Stab}_G(\alpha_i)|}$$

where $\alpha_i \in O_i$. Since $|G| = p^k$, then if $|O_i| > 1$, it follows that $|\mathrm{Stab}_G(\alpha_i)|$ strictly divides p^k, so p divides $|O_i|$. This gives the result:

$$|\Omega| - |\mathrm{Fix}_\Omega(G)| \equiv_p 0$$

□

This has a delightful corollary; a kind of "fixed-point theorem" finding its home in algebra!

Corollary 4. *Let G be a p-group, p prime, acting on finite Ω. If p does not divide $|\Omega|$, then Ω has a point fixed by G; i.e., $|\mathrm{Fix}_\Omega(G)| > 1$.*

After all, if p does not divide $|\Omega|$, then $|\mathrm{Fix}_\Omega(G)| \not\equiv_p 0$.

Let G be a group and p prime so that p divides $|G|$. Let $a_p = \max_a\{p^a \text{ divides } |G|\}$. Then we define:

$$\mathrm{Syl}_p(G) = \{H \leq G : |H| = p^{a_p}\},$$

the set of **Sylow p-subgroups** of G.

We give two concrete examples, one immediate, one interesting.

- Suppose $|G| = p^a m$, where p is prime and does not divide m. Then if $P \leq G$, where $|P| = p^a$, it holds that:

$$P \in \mathrm{Syl}_p(G)$$

- Let $G = S_4$. Since $|G| = 24 = 3 \cdot 2^3$, to find the Sylow 2 and 3-subgroups, we need to find subgroups of order 8 and 3. The latter is easy; note $\langle\sigma\rangle \in \mathrm{Syl}_3(G)$ if $\mathrm{ord}_G(\sigma) = 3$. On the other hand, we recall that the set of symmetry-preserving permutations of the vertices of a square, the group D_4, has order 8, and is contained inside S_4. We can generate it with $\langle(1234), (24)\rangle$, a rotation by $\pi/2$ radians, and a flip along a diagonal. Indeed:

$$D_4 \cong \{a, b : a^4 = e = b^2, bab = a^{-1}\}$$

A natural question is whether every group has a Sylow p-subgroup, if p prime divides $|G|$. So far we have found some, but are we guaranteed their existence? The answer is yes– but first, a technical lemma.

Lemma 3. *Let p be prime, and $n = p^a m$. Then:*

$$\binom{n}{p^a} \equiv_p m$$

In particular, if p does not divide m, then p does not divide $\binom{n}{p^a}$.

Proof. Since $x \mapsto x^p$ is an homomorphism in $\mathbb{Z}/p\mathbb{Z}$, it holds that:

$$(1+x)^n = (1+x)^{p^a m} \equiv_p (1 + x^{p^a})^m$$

Thus mod p, it holds that the coefficient of x^{p^a} in $(1+x)^n$ is the same as the coefficient of x^{p^a} in $(1 + x^{p^a})^m$. By the Binomial Theorem, this is nothing but:

$$\binom{n}{p^a} \equiv_p \binom{m}{1}$$

which is what we wished to show. □

Now we are ready to prove the first of Sylow's Theorems.

Theorem 5 (Sylow's Existence Theorem)**.** *If G is finite and p prime divides $|G|$, then* $\mathrm{Syl}_p(G) \neq \varnothing$.

Proof. There is a proof by induction not unlike Cauchy's Theorem, but we will proceed in a gorgeous proof by group action. We write $|G| = p^a m$, where m is not divisible by p. Let:

$$\Omega = \{X \subseteq G : |X| = p^a\}$$

be the set G acts on by left multiplication. Since $|\Omega| = \binom{n}{p^a}$, Lemma 3 gives that p does not divide $|\Omega|$. Next, decompose Ω as in the general class equation. If $\mathrm{Fix}_\Omega(G)$ is nonempty, we are done; any subset fixed by G would necessarily be a subgroup, and by construction, a Sylow p-subgroup.

So suppose that $\mathrm{Fix}_\Omega(G)$ is empty. Then $|O_i| > 1$ for all orbits O_i, and since p does not divide $|\Omega|$, there is some j so that p does not divide $|O_j|$. Since $|O_j| = (p^a m)/|\mathrm{Stab}_G(X_j)|$, it follows that $|\mathrm{Stab}_G(X_j)| \geqslant p^a$.

To complete the proof, we will show the reverse inequality. Fix $\alpha \in X_j$. If $g \in \mathrm{Stab}_G(X_j)$, then $g \bullet X_j = gX_j = X_j$, so $g\alpha \in X_j$, and hence $\mathrm{Stab}_G(X_j)\alpha \subseteq X$, which gives:

$$|\mathrm{Stab}_G(X_j)| \leqslant |X| = p^a$$

completing the proof. □

In fact, we get something stronger.

Lemma 4. *If $|H| = p^a$, then H has a subgroup of order p^k for $0 \leqslant k \leqslant a$.*

which implies the same result for $G \geq H$ as in Theorem 5.

Proof. In this proof, we let r be the quotient map.

We proceed by induction on $|H|$. The base case is straightforward: $\mathbb{Z}/2\mathbb{Z}$ has two subgroups, $\mathbb{Z}/2\mathbb{Z}$ and $\{e\}$, respectively of order 2^0 and 2^1.

Now suppose $|H| = p^a$. Then by Corollary 3, $Z(H)$ is nontrivial.

There are two cases; either $H = Z(H)$, and $H \neq Z(H)$.

Case 1: $H = Z(H)$.

If $H = Z(H)$, then H is abelian. Fix $0 < k \leqslant a$. Let $h \neq e \in H$, and write $\mathrm{ord}_H(h) = m > 1$. If $m = p^k$, we are done, so assume not.

If p^k divides m, then we can find an element of $\langle h \rangle$ of order p^k.

If p^k does not divide m, then notice that p^k divides $|H/\langle h\rangle|$, so by induction $[x] \in |H/\langle h\rangle|$ so that $\mathrm{ord}_{H/\langle h\rangle}([x]) = p^k$. Thus $x^{p^k} \in \langle h\rangle$, so $x^{p^k} = h^z$ for some $z \in \mathbb{Z}$, hence $x^{p^k m} = e$. Since the quotient map is a homomorphism, p^k divides $\mathrm{ord}_G(x)$. If $x^m = e$, then p^k divides m, which contradicts the case. Thus p^k divides $\mathrm{ord}_H(x)$, and we proceed as in the previous case.

Case 2: $H \neq Z(H)$.

If $H \neq Z(H)$, then let $Z(H) = p^k$ for some $0 < k < a$. Then by induction, $Z(H)$ has a subgroup of order p^l, $0 \leqslant l \leqslant k$, so H has that subgroup of order p^l for such l. On the other hand, consider the quotient $H/Z(H)$. This has order p^{a-k}, and by induction has subgroups of order p^m for $0 \leqslant m \leqslant a-k$. If $G \leq H/Z(H)$, then $|r^{-1}(G)| = |Z(H)||G|$ (indeed, $r^{-1}(G)$ is comprised of $|G|$-many cosets of $|Z(H)|$), which provides subgroups of H of order p^n for $k \leqslant n \leqslant a$. Indeed, to obtain a subgroup of order n, pick the subgroup G of $H/Z(H)$ of order p^{n-k}, and take $r^{-1}(G) \leq H$. □

1.3 1/31/22: Continuing The Suite of Sylow Theorems

In this section, we continue to assume G is finite. This is used whenever we do a size comparison; if $H \leq G$ and $\text{card}(H) = \text{card}(G)$, then $H = G$ always when G is finite. If we care to think about infinite groups, then most of the fundamentals can be recovered by replacing $|G|/|H|$ with $(G : H)$.

Theorem 6 (Sylow's Conjugacy Theorem)**.** *Let Q be a p-subgroup (p prime) of G and P a Sylow p-subgroup of G. Then:*

$$Q \leq xPx^{-1}$$

for some $x \in G$.

That is, up to an automorphism of G, every p-subgroup of G can be found within any Sylow p-subgroup of G.

Proof. Take $\Omega = \{gP : g \in G\}$. Then Q acts on Ω by left multiplication. Notice that $|\Omega| = |G|/|P|$, so using the facts that $G = p^a m$ for some m coprime to p, and $|P| = p^a$, it holds that $\gcd(|\Omega|, p) = 1$.

By fixed-point congruence, Q has a fixed point on Ω. Hence there is some $g \in G$ so that for all $q \in Q$:

$$qgP = gP$$

This is nothing but $g^{-1}qgP = P$, so for all $q \in Q$, $g^{-1}qg \in P$, hence $q \in qPq^{-1}$, so $Q \subseteq gPg^{-1}$. Since $P \leq G$, we conclude $Q \leq gPg^{-1}$. □

Moreover, for G finite we can get a very nice result:

Corollary 5. *If $P, Q \in \text{Syl}_p(G)$, then P and Q are conjugate.*

Proof. By Theorem 6, $Q \leq xPx^{-1}$ for some $x \in G$. However, $|Q| = |P| = |xPx^{-1}|$, so $\leq$ is actually equality. □

Thus if $P \in \text{Syl}_p(G)$, we get a nice representation which lends to computation:

$$\text{Syl}_p(G) = \{xPx^{-1} : x \in G\}$$

To compute this, consider the action of G on its subgroups $\mathcal{S}$ by conjugation. Writing $n_p = |\text{Syl}_p(G)|$, the Orbit-Stabilizer lemma yields:

$$n_p = \frac{|G|}{|\text{Stab}_{\mathcal{S}}(P)|} = \frac{|G|}{|N_G(P)|}$$

We can eke out a little more than this; by the multiplicity of the index, where $P \leq N_G(P)$, and is in fact Sylow p in $N_G(P)$:

$$\frac{|G|}{|P|} = n_p \frac{|N_G(P)|}{|P|}, \text{ hence } n_p = \frac{|G||N_G(P)|}{|P|^2}$$

we see that all factors of p are divided out of n_p. That is to say, the left-hand identity and right-hand identity imply, respectively:

1. $\gcd(n_p, p) = 1$,
2. and n_p divides $|G|/|P|$.

We can with some observation extract one more computational tool:

Theorem 7 (Sylow's Counting Theorem)**.** *Let* $|G| = p^a m$*, where* $\gcd(p, m) = 1$*. Then:*

$$n_p \equiv_p 1$$

Proof. Let P act on $\Omega = \mathrm{Syl}_p(G)$ by conjugation; notice that this is a valid group action only because $\mathrm{Syl}_p(G)$ is a conjugacy class of G, hence P.

By the fixed-point congruence, it suffices to show that $|\mathrm{Fix}_\Omega(G)| \equiv_p 1$. We claim something stronger: that the only fixed point of this action is P. Why is this?

Suppose Q is fixed by P; i.e., $pQp^{-1} = Q$ for all $p \in P$. Then $p \in N_G(Q)$, thus $P \subseteq N_G(Q)$, and since $N_G(Q) \leq G$, it holds that $P \leq N_G(Q)$. By construction, $Q \trianglelefteq N_G(Q)$, so $QP = PQ$, which is necessary and sufficient to conclude that $PQ \leq N_G(Q)$.

Since P, Q are p-groups, it follows that $P \cap Q$ is as well, so $|PQ| = (|P||Q|)/(|P \cap Q|) = p^b$ for some b. In fact, $b = a$. After all, $|Q|/(|P \cap Q|)$ is a power of p, say p^c, so $|PQ| = |P|p^c \geqslant p^a$. Since $P, Q \in \mathrm{Syl}_p(G)$, we know that $|PQ| \leq p^a$, so $|PQ| = p^a$. Since $P, Q \subseteq PQ$, it follows that:

$$P = PQ = Q$$

Thus $\mathrm{Fix}_\Omega(G) = \{P\}$, and we are done. □

Thus we have

Theorem 8 (Suite of Elementary Sylow Theory)**.** *Suppose* G *is finite,* p *prime, and* $|G| = p^a m$ *so that* $\gcd(p, m) = 1$*. Writing* $n_p = |\mathrm{Syl}_p(G)|$*:*

1. $\mathrm{Syl}_p(G) \neq \varnothing$,
2. $\mathrm{Syl}_p(G)$ *is a conjugacy class of* G,
3. *Any* p*-subgroup is contained in some Sylow* p*-subgroup of* G
4. $\gcd(n_p, p) = 1$,
5. n_p *divides* $|G|/|P|$,
6. *and* $n_p \equiv_p 1$.

This is remarkably powerful; in particular, this allows quick progress in understanding G's group structure, given information about G's Sylow p-subgroups. Here are two examples.

1. Simplicity Test 1: If $n_p = 1$, then G is not simple. This is because the only element of $\mathrm{Syl}_p(G)$ is its own conjugacy class, hence is normal.

2. Simplicity Test 2: Suppose $|G| = pq$, where $p < q$ are distinct primes. Since n_q divides p, either $n_q = p$ or 1. Since $n_q \equiv_q 1$, q divides $n_q - 1$. If $n_q = p$, then q would divide $p - 1$, which is impossible, since $p < q$. Thus $n_q = 1$, and $Q = \mathrm{Syl}_q(G) \trianglelefteq G$.

We also can use Sylow p-subgroups for decompositions:

Theorem 9 (Frattini's Argument)**.** *Suppose G is a group and $M \triangleleft G$. Let $P \in \mathrm{Syl}_p(M)$. Then:*

$$G = N_G(P)M$$

Chapter 2

The Jordan Canonical Form

2.1 Remark

Here should be a series of linear-algebraic notes on the Jordan Canonical Form. I couldn't make head nor tail of the lecture, so I am omitting them until they can be cleared.

But fear not! On page 74 there is a *slick* (and more natural) second proof of existence and uniqueness of the canonical form. It uses the heavy weight of the Structure Theorem for f.g. Modules over PID's, but in this case we use the theorem as a scalpel, not a sledghammer.

2.2 Bonus: Computing the Jordan Canonical Form

Although I can't make too much sense of (the omitted) first proof of the Jordan Canonical Form, it is sensible to have some working knowledge. Here is an algorithm, which will not be proven to work. Given a matrix A:

1. Find $\chi_A(x) = \prod_{i=1}^{k}(x-\lambda_i)^{\alpha_i}$, the characteristic polynomial of A.
2. From this, we can determine the Jordan canonical form J directly. For each λ_i:
   (a) The algebraic multiplicity α_i of λ_i is the total number of appearances of λ_i on the diagonal of J.
   (b) The geometric multiplicity $\dim\ker(A-\lambda_i I)$ of λ_i is the total number of Jordan blocks in λ_i. More generally, the number of Jordan blocks of size k in λ_i is:
   $$2\dim\ker[(A-\lambda_i I)^k] - \dim\ker[(A-\lambda_i I)^{k-1}]\dim\ker[(A-\lambda_i I)^{k-1}]$$
3. At the end of the day, we will have $\dim\ker(A-\lambda_i I) = m$-many Jordan blocks in λ_i. We find a basis $\{\mathbf{b}_1,\ldots,\mathbf{b}_m\}$ of $\ker(A-\lambda_i I)$, and then create a Jordan chain for each $\mathbf{b}_i$, where we define:
   $$\begin{cases}\mathbf{b}_i^{(0)} = \mathbf{b}_i \\ \mathbf{b}_i^{(j+1)} \text{ is such that } (A-\lambda_i I)\mathbf{b}_i^{(j+1)} = \mathbf{b}_i^{(j)}\end{cases}$$
   It is significant that if there are multiple blocks in λ_i, we need to make sure to choose $\mathbf{b}_i^{(j+1)}$ to be linearly independent of *all the vectors chosen thus far.*
   We will not prove this, but for each i this process will eventually terminate (i.e., the according Gaussian elimination will resolve as inconsistent), and we will have as many chains of length l as there are Jordan blocks of size l in λ_i.
4. Arrange the chains each increasing in (j), consistent with the sizes of the according Jordan blocks in J.
5. Concatenate these chains for each λ_i to obtain the similarity matrix S so that:
   $$A = SJS^{-1}$$

Here is an example, in the nilpotent case. Let:

$$A = \begin{bmatrix}0 & 0 & 0 & 0\\ 0 & 1 & 1 & -1\\ 0 & -1 & -1 & 1\\ 0 & 0 & 0 & 0\end{bmatrix}$$

Then $\chi_A(x) = x^4$, so the only eigenvalue is 0 of algebraic multiplicity 4. The geometric multiplicity of 0 is 3, so there are three blocks. This allows us to see that there will

be two blocks of size 1, and one block of size 2 (we can use the direct equation normally, but in this case a pigeonhole argument is quicker).

We construct a basis of $\ker(A)$:

$$\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\} = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ -1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \right\}$$

Observe there are no $\mathbf{x}$ so that $A\mathbf{x} = \mathbf{b}_1$ and $A\mathbf{x} = \mathbf{b}_3$; hence their chain terminates, and so they correspond each to a Jordan block of size 1 in 0.

We row reduce $A\mathbf{b}_2^{(1)} = \mathbf{b}_2^{(0)}$ to obtain the augmented matrix:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Hence $\mathbf{b}_2^{(1)}$ is of the form:

$$\begin{bmatrix} 0 \\ -1 \\ 0 \\ 0 \end{bmatrix} + \alpha\mathbf{b}_1 + \beta\mathbf{b}_2 + \gamma\mathbf{b}_3$$

We need to choose α, β, γ so that $\mathbf{b}_2^{(1)}$ is independent of $\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$. A suitable choice is:

$$\begin{cases} \alpha = 0 \\ \beta = 1 \\ \gamma = 0 \end{cases}$$

and according the algorithm, we can write:

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & -2 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} \mathbf{0} & 0 & 0 & 0 \\ 0 & \mathbf{0} & 0 & 0 \\ 0 & 0 & \mathbf{0} & \mathbf{1} \\ 0 & 0 & \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & -2 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}^{-1}$$

where the Jordan block elements are bolded.

Chapter 3

Elementary Representation Theory

3.1 2/11/22: Fundamental Constructions of Representation Theory

Suppose that V is a vector space over $\mathbb{K}$. We will write $GL(V)$ for the **group of $\mathbb{K}$-linear isomorphisms of V**.

If $V = \mathbb{C}^n$, it's well-known that $GL(V) \cong GL_n(\mathbb{C})$.

Here is the major definition: given a G a group, $\mathbb{K}$ a field, and V a vector space over $\mathbb{K}$, we say that a group homomorphism:

$$\mathscr{R} : G \to GL(V)$$

is a **representation** of G. Unless we specify elsewhere, we will assume $\mathbb{K} = \mathbb{C}$.

If $\mathscr{R} : G \to GL_n(\mathbb{C})$ is a representation, we say that n is the **dimension** (or **degree**) of the representation.

Two examples of representations are the **trivial representation**, in which $\mathscr{R}(g) = I$ for all $g \in G$, and a representation of $\mathbb{Z}/n\mathbb{Z}$ with the the rotation matrices of angle $2q\pi/n$ for $1 \leqslant q \leqslant n$.

The trivial representation isn't super interesting. We say that a representation of G is **faithful** if $\ker(f) = f^{-1}(I) = \{e\}$. In other words, f is injective. The choice of 'faithful' is telling— a nonfaithful representation is harder to work with.

In general, if the kernel of $\mathscr{R}$ is $H \leq G$, by the universal property of the group quotient we can always obtain a representation $\mathscr{R}'$ of G/H which is faithful.

Another general construction is the direct sum. Given $\mathscr{R}_1 : G \to GL(V_1)$ and $\mathscr{R}_2 : G \to GL(V_2)$ representations, we can represent their **direct sum**:

$$(\mathscr{R}_1 \oplus \mathscr{R}_2) : G \to GL(V_1 \oplus G_2)$$

which acts coordinatewise:

$$(\mathscr{R}_1 \oplus \mathscr{R}_2)(g) \begin{bmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \end{bmatrix} = \begin{bmatrix} \mathscr{R}_1(g)\mathbf{v}_1 \\ \mathscr{R}_2(g)\mathbf{v}_2 \end{bmatrix}$$

If $V_1 = \mathbb{C}^n$ and $V_2 = \mathbb{C}^m$, this is nothing but the observation that $(\mathscr{R}_1 \oplus \mathscr{R}_2)(g)$ takes a block-diagonal form:

$$g \mapsto \begin{bmatrix} \mathscr{R}_1(g) & \mathbf{0} \\ \mathbf{0} & \mathscr{R}_2(g) \end{bmatrix}$$

Since representations essentially live in a vector space, we need to consider them equivalent modulo vector space isomorphism. Indeed, $\mathscr{R}_1 : G \to GL(V_1)$ and $\mathscr{R}_2 : G \to GL(V_2)$ are said to be **isomorphic** if there is an isomorphism:

$$i : V_1 \to V_2$$

so that for all $g \in G$ and $\mathbf{v} \in V_1$:

$$i(\mathscr{R}_1(g)\mathbf{v}_1) = \mathscr{R}_2(g)(i(\mathbf{v}))$$

If $V_1 = V_2 = \mathbb{C}^n$, all such isomorphisms are conjugation by invertible linear maps; i.e., nonsingular matrices, so in this case the two representations are isomorphic if there is some uniform φ linear bijective so that:

$$\mathscr{R}_2(g) = \varphi^{-1}\mathscr{R}_1(g)\varphi$$

We say that a representation $\mathscr{R}$ is **decomposable** if it is isomorphic to a direct sum of positive-dimensional representations. If this is not the case, we say that $\mathscr{R}$ is **indecomposable**.

It's not hard to see that if $V = \mathbb{C}^n$, this is equivalent to there being a change of basis so that $\mathscr{R}(g)$ is block-diagonal for all $g \in G$. It's also fairly straightforward that:

Theorem 10. *Every finite-dimensional representation of G is isomorphic to a direct sum of some number of indecomposable representations.*

As easy as this is to see, proving it is not easy. We will return to this in a later section.

Given a representation $\mathbb{R} : G \to GL(V)$, if there is some subspace $W \subseteq V$ that is closed under action of $f(g)$; i.e.:

$$f(g)(W) \subseteq W$$

for all $g \in G$, then we say that W is a **G-invariant** (or otherwise **invariant**) subspace of V. If there is a G-invariant subspace W, we can construct a **subrepresentation** $\mathscr{R}|_W : G \to GL(W)$ given by $g \mapsto \mathscr{R}(g)|_W$.

How does this look in $GL_n(\mathbb{C})$? Consider a basis of W, and extend it to a basis $\mathscr{B}$ of V. In other words, write $V = W \oplus Z$ for some $Z \subseteq V$. Supposing the basis of W has m vectors, then we can break up the expression of $\mathscr{R}(g)$ in this basis into a block matrix:

$$\begin{bmatrix} R_{11} & R_{12} \\ R_{21} & R_{22} \end{bmatrix}$$

where R_{11} is $m \times m$. If any vector $\mathbf{w}$ is in W, then in this basis it is of the form $(\mathbf{w}_1, \mathbf{0})^t$. Thus by matrix multiplication:

$$\begin{bmatrix} R_{11} & R_{12} \\ R_{21} & R_{22} \end{bmatrix} \begin{bmatrix} \mathbf{w}_1 \\ \mathbf{0} \end{bmatrix} = \begin{bmatrix} R_{11}\mathbf{w}_1 \\ R_{21}\mathbf{w}_1 \end{bmatrix}$$

hence $R_{21} = \mathbf{0}$, or else $\mathscr{R}(g)\mathbf{w} \notin W$. That is to say:

$$\mathscr{R}(g) = \begin{bmatrix} \mathscr{R}(g)|_W & R_{12} \\ \mathbf{0} & R_{22} \end{bmatrix}$$

since $\mathscr{R}(g)|_W$ is the representation restricted to W.

This class is worth naming: a representation is **reducible** if it has a nontrivial subrepresentation. If not, it is called **irreducible**.

Our next major project is to prove a fundamental tool in finite group representation theory:

Theorem 11 (Maschke's Theorem)**.** *Every reducible complex representation of a finite group is decomposable.*

This is decidably false even for the simplest infinite groups. Indeed, given $A \in GL_n(\mathbb{C})$, there is a representation:

$$\mathscr{R}_A : \mathbb{Z} \to GL_n(\mathbb{C})$$

given by $\mathscr{R}_A(n) = A^n$. If we pick $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, we can see that there is a nontrivial $\mathbb{Z}$-invariant subspace: $\text{span}(\mathbf{e}_1)$. Thus $\mathscr{R}_A$ is reducible, but contrary to the statement of Maschke's Theorem, it is not decomposible. If it were, A would be diagonalizable— but A is clearly its own Jordan canonical form, so this is not the case.

We shall prove Maschke's Theorem later; for now, we describe another construction.

Like all algebraic objects, vector spaces have a nice quotient object. Given any subspace $N \subseteq V$, we can obtain the quotient space V/N of the underlying additive group, with the rule $\lambda[\mathbf{x}] = [\lambda\mathbf{x}]$ for all scalars λ, where $[-]$ denotes the projection $V \to V/N$.

To get a quotient representation in the quotient vector space, we need a little more: it is necessary for N to be G-invariant.

That is, given $\mathscr{R} : G \to GL(V)$ a representation and $W \subseteq V$ invariant, we can construct a **quotient representation**:

$$\mathscr{R}/W : G \to GL(V/W)$$

by the rule $\mathscr{R}/W(g)[\mathbf{v}] = [\mathscr{R}(g)\mathbf{v}]$, where $[-]$ denotes the projection $V \to V/W$. We need to check that each map is well-defined; suppose $[\mathbf{a}] = [\mathbf{b}]$. Then $\mathbf{a} = \mathbf{b} + \mathbf{w}$, where $\mathbf{w} \in W$.

Then

$$\mathscr{R}/W(g)[\mathbf{a}] = [\mathscr{R}(g)\mathbf{a}] = [\mathscr{R}(g)\mathbf{b} + \mathscr{R}(g)\mathbf{w}] = [\mathscr{R}(g)\mathbf{b} + \mathbf{w}'] = \mathscr{R}/W(g)[\mathbf{b}],$$

where $\mathbf{w}' \in W$ since W is G-invariant.

How does this look in $GL_n(\mathbb{C})$? Again write $V = W \oplus Z$ for some $Z \subseteq V$. Then:

$$\mathscr{R}(g) = \begin{bmatrix} \mathscr{R}(g)|_W & R_{12} \\ \mathbf{0} & R_{22} \end{bmatrix}$$

If we take $\mathbf{v} \in V$, we can write it $(\mathbf{w}, \mathbf{z})$, and compute:

$$\mathscr{R}(g) \begin{bmatrix} \mathbf{w} \\ \mathbf{z} \end{bmatrix} = \begin{bmatrix} \mathscr{R}(g)|_W & R_{12} \\ \mathbf{0} & R_{22} \end{bmatrix} \begin{bmatrix} \mathbf{w} \\ \mathbf{z} \end{bmatrix} = \begin{bmatrix} \mathscr{R}(g)|_W\mathbf{w} + R_{12}\mathbf{z} \\ R_{22}\mathbf{z} \end{bmatrix}$$

Since $[\mathscr{R}(g)|_W\mathbf{w} + R_{12}\mathbf{z}] = [0]$, it follows that in the quotient representation:

$$\mathscr{R}/W(g)\mathbf{z} = R_{22}\mathbf{z},$$

so given a reducible representation $\mathscr{R}$ with G-invariant subspace W, we can write:

$$\mathscr{R}(g) = \begin{bmatrix} \mathscr{R}(g)|_W & R_{12} \\ \mathbf{0} & \mathscr{R}/W(g) \end{bmatrix}$$

where $\mathscr{R}(g)|_W$ is the subrepresentation with respect to W, and $\mathscr{R}/W(g)$ is the quotient representation with respect to W.

3.2 2/14/22: Representation Theory: Notions in Linear Algebra

Suppose that V is a vector space over some field $\mathbb{K}$, and suppose V_1 and V_2 are subspaces of V. Then we say that V_1 and V_2 are **complements**, or **complementary subspaces** if every $\mathbf{v} \in V$ can be uniquely expressed as $\mathbf{v}_1 + \mathbf{v}_2$, where $\mathbf{v}_1 \in V_1$ and $\mathbf{v}_2 \in V_2$. Call this a **complementary representation**.

In finite dimensions, complements are as well-behaved as one would expect:

Lemma 5. *Suppose V is finite-dimensional, and V_1 and V_2 are subspaces. Then the following conditions are equivalent:*

1. *V_1 and V_2 are complements.*
2. *$V_1 \cap V_2 = \{\mathbf{0}\}$ and $(V_1 \oplus V_2) = V$.*
3. *If $\mathscr{B}_1$ is a basis of V_1 and $\mathscr{B}_2$ is a basis of V_2, then $\mathscr{B}_1 \cup \mathscr{B}_2$ is a basis of V.*
4. *There exists bases $\mathscr{B}_1$ of V_1 and $\mathscr{B}_2$ of V_2 such that $\mathscr{B}_1 \cup \mathscr{B}_2$ is a basis of V.*

Proof. First we show (1) $\implies$ (2).

Suppose $\mathbf{v} \in V_1 \cap V_2$. If $\mathbf{v} \neq \mathbf{0}$, then we can represent $\mathbf{v} = \mathbf{v} + \mathbf{0} = \mathbf{0} + \mathbf{v}$, where the first element of the sum is in V_1, and the second is V_2. This contradicts uniqueness of complementary representation. Thus for all $\mathbf{v} \in V$, we have a unique decomposition $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2$, which is a linear combination of elements of V_1 and V_2; i.e., $(V_1 \oplus V_2) = V$.

Now we show (2) $\implies$ (3). Suppose $\mathscr{B}_1 = \{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ is a basis of V_1, and $\mathscr{B}_2 = \{\mathbf{w}_1, \dots, \mathbf{w}_m\}$ is a basis of V_2. We wish to show that $\mathscr{B}_1 \cup \mathscr{B}_2$ is a basis of V. Suppose that there is a linear combination:

$$a_1\mathbf{v}_1 + \cdots + a_k\mathbf{v}_k = -b_1\mathbf{w}_1 + \cdots - b_m\mathbf{w}_m$$

Since both sides of the expression are in $V_1 \cap V_2$, it follows that both are $\mathbf{0}$. Using that $\mathscr{B}_1$ and $\mathscr{B}_2$ are linearly independent, it follows that $a_i = 0$ and $b_i = 0$ for all i, so $\mathscr{B}_1 \cup \mathscr{B}_2$ is linearly independent.

Since $(V_1 \cup V_2) = V$, every element of $\mathbf{v}$ is a linear combination of some vectors in V_1 and V_2. Expressing these in terms of $\mathscr{B}_1$ and $\mathscr{B}_2$ give an expression of $\mathbf{v}$ in terms of $\mathscr{B}_1 \cup \mathscr{B}_2$; i.e., $(\mathscr{B}_1 \cup \mathscr{B}_2) = V$, hence $\mathscr{B}_1 \cup \mathscr{B}_2$ is a basis.

To see (3) $\implies$ (4), observe that every vector space has a basis.

Last, we show (4) $\implies$ (1). Suppose that there are bases $\mathscr{B}_1 = \{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ of V_1 and $\mathscr{B}_2 = \{\mathbf{w}_1, \dots, \mathbf{w}_m\}$ of V_2 so that $\mathscr{B}_1 \cup \mathscr{B}_2$ is a basis of V. We wish to show that $\mathbf{v}$ has a unique complimentary representation. Thus assume:

$$\begin{cases} \mathbf{v} = \mathbf{u} + \mathbf{w} & \mathbf{u}, \mathbf{u}' \in V_1 \\ \mathbf{v} = \mathbf{u}' + \mathbf{w}' & \mathbf{w}, \mathbf{w}' \in V_2 \end{cases}$$

Then $\mathbf{0}$ has the complimentary representation $(\mathbf{u} - \mathbf{u}') + (\mathbf{w} - \mathbf{w}')$, and so:

$$\mathbf{u} - \mathbf{u}' = a_1\mathbf{v}_1 + \cdots + a_k\mathbf{v}_k$$

$$\mathbf{w} - \mathbf{w}' = b_1\mathbf{w}_1 + \cdots + a_m\mathbf{w}_m$$

for some a_i, b_i. Hence:

$$\mathbf{0} = a_1\mathbf{v}_1 + \cdots + a_k\mathbf{v}_k + b_1\mathbf{w}_1 + \cdots + b_m\mathbf{w}_m$$

and using that $\mathscr{B}_1 \cup \mathscr{B}_2$ is a basis, it follows that $a_i = 0$ and $b_i = 0$ for all i. Thus $\mathbf{u} = \mathbf{u}'$ and $\mathbf{w} = \mathbf{w}'$, finishing the lemma.

□

As is usually the case in linear algebra, a subspace-oriented construction has a corresponding notion in the world of linear maps. We say that L is **idempotent** if $L^2 = L$.

Theorem 12. *There is a natural bijection between idempotent linear maps and ordered pairs of complementary subspaces of V. The explicit bijection is as follows. If $L^2 = L$, then* $\mathrm{im}L$ *and* $\ker L$ *are complements. For the inverse bijection, we project $\mathbf{v} \in V$ onto V_1 along V_2, which is clearly linear idempotent.*

Proof. Suppose $L^2 = L$. Write $V_1 = \mathrm{im}L$ and $V_2 = \ker L$, and let $\mathbf{v} \in V_1 \cap V_2$. Since $\mathbf{v} \in V_1$, it holds that there is some $\mathbf{w}$ so that $\mathbf{v} = L\mathbf{w}$. Since $\mathbf{v} \in V_2$, we also know that $L\mathbf{v} = \mathbf{0}$.

Using idempotency:

$$\mathbf{v} = L\mathbf{w} = L^2 = L(L\mathbf{w}) = L\mathbf{v} = \mathbf{0}$$

This fulfils the first criterion for complementation. We claim the complementary representation is:

$$\mathbf{v} = L\mathbf{v} + (I - L)\mathbf{v}$$

Indeed, $L\mathbf{v} \in V_1$. To see that $(I - L)\mathbf{v} \in V_2$, observe that:

$$L(I - L)\mathbf{v} = (L - L^2)\mathbf{v} = \mathbf{0}\mathbf{v} = \mathbf{0}$$

which completes the first part of the proof. On the other hand, suppose V_1, V_2 are complements. Define $L(\mathbf{v})$ to be the projection onto V_1 along V_2; i.e., $L(\mathbf{v})$ is the unique $\mathbf{v}_1$ so that $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2$, where $\mathbf{v}_1 \in V_1$ and $\mathbf{v}_2 \in V_2$.

To see that L is linear, suppose $\mathbf{v}, \mathbf{v}' \in V$. Then with the respective complementary representations, $\mathbf{v}+\mathbf{v}' = (\mathbf{v}_1+\mathbf{v}_1')+(\mathbf{v}_2+\mathbf{v}_2')$. Thus $L(\mathbf{v}+\mathbf{v}') = \mathbf{v}_1+\mathbf{v}_1' = L(\mathbf{v})+L(\mathbf{v}')$. Likewise, if $c \in \mathbb{K}$, $L(c\mathbf{v}) = c\mathbf{v}_1 = cL(\mathbf{v})$.

Idempotency is not hard to see. For all $\mathbf{v} \in V$, it holds that $L(\mathbf{v}) = \mathbf{v}_1$, and $L^2(\mathbf{v}) = L\mathbf{v}_1 = \mathbf{v}_1$ (since $\mathbf{v}_1 \in V_1$. Therefore $L^2 = L$.

It is easy to see that these two maps are inverses. □

With this theory, we can talk about representation theory.

Theorem 13 (Maschke's Theorem)**.** *Suppose that G is a finite group, and $\mathscr{R} : G \to \mathrm{Aut}(V) \cong GL_n(\mathbb{C})$ is a representation. Moreover, suppose that $\{\mathbf{0}\} \neq V_1 \subsetneq V$ is a G-invariant subspace. Then there exists $V_2 \subsetneq V$ G-invariant so that V_1 and V_2 are complements.*

One proof of Theorem 13 uses Theorem 12 and some clever averaging over an idempotent map conjugated by $f(g)$ for each $g \in G$. Frankly, I didn't understand the proof, and there's another proof coming up that does a better job of pulling back the curtain; it turns out that Maschke's theorem practically comes for free with some theory about how "nice" a representation of a finite group can be, and how such "nice" representations can be decomposed.

3.3 2/16/22: Bilinear Algebra Fundamentals

Let V be a vector space over $\mathbb{K}$. A **bilinear form** on V is some $F : V^2 \to \mathbb{K}$ which is linear in each coordinate. The well-known example is the dot product on $\mathbb{R}^d$. In this sense, bilinear forms allow for "multiplication" in a vector space.

However, we can come up with more examples very easily. Let's assume $\mathbb{K} = \mathbb{R}$, and suppose A is $n \times n$. Then we can obtain a bilinear form:

$$f_A(\mathbf{x}, \mathbf{y}) = \mathbf{y}^t A \mathbf{x}$$

It is not hard to see that if $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a basis for $\mathbb{R}^d$, and A is written in that basis, then the coefficient of the term $x_i y_j$ is a_{ji}. In fact, this works in the reverse as well!

Suppose that F is bilinear on V, and $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ is a basis of V. Then writing:

$$\mathbf{x} = x_1 \mathbf{v}_1 + \cdots + x_k \mathbf{v}_k$$

and

$$\mathbf{y} = y_1 \mathbf{v}_1 + \cdots + y_k \mathbf{v}_k$$

it follows that:

$$F(\mathbf{x}, \mathbf{y}) = \sum_{i,j=1}^{k} F(\mathbf{v}_i, \mathbf{v}_j) x_i y_j$$

So if we define $(A)_{ij} = F(\mathbf{v}_j, \mathbf{v}_i)$, it holds that $F(\mathbf{x}, \mathbf{y}) = \mathbf{y}^t A \mathbf{x}$.

We say a bilinear form is **symmetric** if for all $\mathbf{x}, \mathbf{y}$, it holds that $F(\mathbf{x}, \mathbf{y}) = F(\mathbf{y}, \mathbf{x})$. The refinement of the above bijection is stated in terms of quadratic functions.

A **quadratic function** on V is some $f : V \to \mathbb{R}$ such that $f(\mathbf{x}) = F(\mathbf{x}, \mathbf{x})$ for some bilinear F.

For example, if $F(\mathbf{x}, \mathbf{y}) = \mathbf{y}^t \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \mathbf{x}$, the associated quadratic function is $f(\mathbf{x}) = x_1^2 + 5x_1x_2 + 4x_2^2$.

As alluded to, there is a meaningful bijection between quadratic functions on V and symmetric bilinear forms on V.

Proof. The backwards map is straightforward. Given a symmetric bilinear form F, define $f(\mathbf{x}) = F(\mathbf{x}, \mathbf{x})$. The reverse is true as well. Given $f(\mathbf{x}) = F(\mathbf{x}, \mathbf{x})$, we can just take the symmetric and antisymmetric parts of F as follows:

$$F(\mathbf{x}, \mathbf{y}) = \frac{F(\mathbf{x}, \mathbf{y}) + F(\mathbf{y}, \mathbf{x})}{2} + \frac{F(\mathbf{x}, \mathbf{y}) - F(\mathbf{y}, \mathbf{x})}{2}$$

and observe that only the symmetric part contributes to $F(\mathbf{x}, \mathbf{x})$. Thus if a quadratic function is defined by a bilinear form, its "preimage;" i.e., the parts of the form which contribute to $F(\mathbf{x}, \mathbf{y})$ produces the same quadratic form.

□

Intriguingly, this does not work in characteristic 2. Thus the study of quadratic functions in over fields of characteristic 2 is somewhat more fraught than fields of nicer characteristics.

If we work over $\mathbb{R}$, we have the advantage of being able to naively speak of order. A bilinear form $F : V^2 \to \mathbb{R}$ is **positive-definite** if $F(\mathbf{x}, \mathbf{x}) > 0$ for all $\mathbf{x} \neq \mathbf{0}$. We say that F is **positive-semidefinite** if $F(\mathbf{x}, \mathbf{x}) \geqslant 0$ for all $\mathbf{x} \in V$.

Since such forms correspond to matrices, we extend this definition and say that A is **positive-definite** if $\mathbf{x}^t A\mathbf{x} > 0$ for all $\mathbf{x} \neq \mathbf{0}$.

However, to speak of matrices is to imply a choice of basis. When we represent linear functions by matrices, linear isomorphisms (i.e., change of bases) are represented by conjugation by invertible matrices. What is the analogous representation for symmetric bilinear forms?

Evidently, $A \to J^{-1}AJ$ will not always work, since the result matrix may not be symmetric. On the other hand, J^tAJ is always symmetric, if A is! Indeed, suppose that we change our basis; then $\mathbf{x} \mapsto J\mathbf{x}$. Hence:

$$\mathbf{x}^t A\mathbf{x} \mapsto (J\mathbf{x})^t A(J\mathbf{x}) = \mathbf{x}^t(J^tAJ)\mathbf{x}$$

It is extra nice when J is **orthogonal**; i.e., when $J^{-1} = J^t$.

Earlier we discussed the preferred representative of each orbit under conjugation by $GL_n(\mathbb{C})$: the Jordan canonical form. What about the action of $GL_n(\mathbb{R})$ on the real symmetric matrices by transpose-conjugation; i.e.:

$$M \cdot A = M^tAM$$

The answer is surprisingly tight.

Theorem 14 (Sylvester?)**.** *For every symmetric real matrix A, there exists an invertible real matrix J so that J^tAJ is diagonal, with k 1's, m -1's, and $n-k-m$ 0's on the diagonal. Moreover, the number of 1's, -1's, and 0's does not depend on J.*

We call the triplet $(k, m, n-k-m)$ or (k, m) the **signature** of A.

Proof. From a matrix algebra perspective, this is not too hard to see: simply use the fact that real-symmetric A is orthogonally diagonalizable to obtain $A = O^t\Lambda O$, and let $J = OL$ for L an appropriate scaling action.

Indeed, it's not hard to pick L; just let $(L)_{ii} = \frac{1}{\sqrt{|\lambda_i|}}$.

However, we can consider this a question of quadratic functions as well. Indeed, it holds that $F(\mathbf{v}_i, \mathbf{v}_i) = \lambda_i$, so $F(\mathbf{v}_i/\sqrt{|\lambda_i|}, \mathbf{v}_i/\sqrt{|\lambda_i|}) = \pm 1$.

A concrete example shows how we can interpret this problem entirely in terms of quadratic functions. Suppose we wish to compute the signature of:

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

By definition of the associated quadratic function:

$$f(\mathbf{x}) = x_1^2 + 6x_1x_2 + 4x^2$$

Then the essence of the algorithm is to complete the square as we iterate up the index, with an occasional change of basis to avoid any issues. Then at the end, we change the basis for each squared term.

$$x_1^2 + 6x_1x_2 + 4x^2 = (x_1 + 3x_2)^2 - 5x_2^2 = (x_1 + 3x_2)^2 - (\sqrt{5}x_2)^2$$

with the change of basis $x_1 + 3x_2 = y_1$ and $\sqrt{5}x_2 = y_2$, it holds that $F(\mathbf{y}) = y_1^2 - y_2^2$, which corresponds to the reduction we wanted!

$$A \sim \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

To show uniqueness is more theoretical. In fact, if (k, m) is A's signature, it holds that k is the maximal dimension of the subspace on which A's associated quadratic form f_A is positive. After all, in some basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, it holds that $f_A(\mathbf{v}_i) = B_{ii} = 1$ for $i \in 1, \ldots, k$. Thus the maximal dimension on which f_A is positive-definite is at least k.

On the other hand, we can also find an $(n - k)$-dimensional subspace V on which f_A is negative-semidefinite, by the same token. By dimension-counting, if the subspace U on which f_A is positive-definite has dimension exceeding k, it must be the case that $U \cap V \neq \{\mathbf{0}\}$. But then for $\mathbf{x} \neq \mathbf{0} \in U \cap V$:

$$0 < f_A(\mathbf{x}) \leqslant \mathbf{0}$$

which is impossible. □

There is a nice characterization of positive-definite matrices:

Theorem 15 (Sylvester's Criterion)**.** *Suppose that A is a symmetric real matrix. Then the following are equivalent:*

1. *A is positive-definite,*
2. *For every subset of indices of $[n]$, the corresponding principal minor is positive, and*
3. *For every contiguous subset $\{1, \ldots, k\} \subseteq [n]$, the corresponding principal minor is positive.*

Proof. First we show (1) $\implies$ (2). If A is positive definite, then by Theorem 14, it is transpose-similar to I. That is, there is some J so that:

$$J^t A J = I$$

Thus $\det(A)(\det(J))^2 = 1$, thus $\det(A) > 0$. This reasoning applies to every principal minor; just take a restriction of the action.

The implication (2) $\implies$ (3) is immediate.

To show (3) $\longrightarrow$ (1), we will perform induction on the size of A. If A is 1×1, this is immediate.

If A is $n \times n$, the principal minor induced by $[n-1]$ is positive. Thus the signature of A is one of:

$$(n+1, 0), (n, 1), (n, 0)$$

Suppose that:

$$J^t A J = \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & b \end{bmatrix}$$

for some $b \in \{0, 1, -1\}$. Again we observe that $(\det(J))^2 \det(A) = b$, and since $\det A$ is positive, it must be that $b = 1$. $\square$

All of this has been over $\mathbb{R}$. The natural analog to $\mathbb{C}$ is bilinear forms or symmetric matrices, since $\mathbb{C}$ is not totally ordered. Instead, we have sesquilinear forms and Hermitian metrices.

We say that $F : V^2 \to \mathbb{C}$ is a **sesquilinear form** if it is linear in the first component, and "1/2-linear" in the second:

$$F(\mathbf{x}, \mathbf{y}_1 + \lambda \mathbf{y}_2) = F(\mathbf{x}, \mathbf{y}_1) + \overline{\lambda} F(\mathbf{x}, \mathbf{y}_2)$$

for any $\lambda \in \mathbb{C}$. The prototypical example is the complex dot product:

$$F(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} x_i \overline{y_i}$$

From this, we can obtain an analog of positive-definiteness:

$$F(\mathbf{x}, \mathbf{x}) = \sum_{i=1}^{n} |x_i|^2 \in \mathbb{R}_{>0}$$

when $\mathbf{x} \neq \mathbf{0}$.

3.4 2/18/22: Complex Linear and Bilinear Algebra Fundamentals

The notions of bilinearity and symmetry are, as mentioned, not good enough when the field we work over is larger than $\mathbb{R}$. This motivates a new definition; we say that a sesquilinear form F is **Hermitian** if for all $\mathbf{x}, \mathbf{y} \in \mathbb{C}^n$:

$$F(\mathbf{y}, \mathbf{x}) = \overline{F(\mathbf{x}, \mathbf{y})}$$

For any $A \in M_n(\mathbb{C})$, it holds that $F(\mathbf{x}, \mathbf{y}) = \mathbf{y}^* A\mathbf{x}$ is a sesquilinear form, and if F is Hermitian, then it holds that $A^* = A$. Thus we circumvent the process of translation and say outright that $A \in M_n(\mathbb{C})$ is **Hermitian** if $A^* = A$.

Of course, this bijection runs the other way; given a basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ of $\mathbb{C}^n$ and F sesquilinear on $\mathbb{C}^n$, one can define:

$$A = (F(\mathbf{v}_i, \mathbf{v}_j))^*$$

Observe that if F is Hermitian, it holds that $F(\mathbf{x}, \mathbf{x}) = \overline{F(\mathbf{x}, \mathbf{x})}$, so $F(\mathbf{x}, \mathbf{x}) \in \mathbb{R}$, and we can talk about orderings. If Hermitian F satisfies $F(\mathbf{x}, \mathbf{x}) > 0$ for all $\mathbf{x} \neq \mathbf{0}$, we say that it is **positive-definite**. If $A \in M_n(\mathbb{C})$ is Hermitian such that $\mathbf{x}^* A\mathbf{x} > 0$ for all $\mathbf{x} \neq \mathbf{0}$, we also say that A is **positive-definite**.

Hermitian matrices are the right generalization of symmetric matrices. However, another valuable class of $\mathbb{R}$-valued matrices are orthogonal matrices: those M so that $M^t = M^{-1}$. The complex generalization of this class is the obvious one, albeit by a new name: we say that $A \in M_n(\mathbb{C})$ is **unitary** if $A^* = A^{-1}$.

Why unitary? If $A^* = A^{-1}$, then $\det(A)^{-1} = \overline{\det(A)}$, so $\det(A) \in S^1 \subseteq \mathbb{C}$.

We write $U(n)$ for the group of $n \times n$ unitary matrices, and $SU(n)$ for the group of $n \times n$ unitary matrices of determinant 1. In fact, $SU(n)$ is rather cute.

1. For $n = 1$, it is not hard to see that $SU(1) = \{1\}$.

2. The case $n = 2$ is surprising. If:

$$M = \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix}$$

is in $SU(2)$, then by the fact that $M^* M = I$, we obtain the following system of equations:

$$\begin{cases} \alpha\overline{\gamma} + \beta\overline{\delta} = 0 \\ |\alpha|^2 + |\beta|^2 = 1 \\ |\gamma|^2 + |\delta|^2 = 1 \end{cases}$$

If we fix α and β, the first line expresses that (γ, δ) is proportional to $(-\overline{\beta}, \overline{\alpha})$. Hence:

$$M = \begin{bmatrix} & -\overline{\beta}u \\ \beta & \overline{\alpha}u \end{bmatrix}$$

for some $u \neq 0$ in $\mathbb{C}$.

By substitution in the third equation above, $|u| = 1$, and by using the fact that $\det(M) = 1$ for the second expression of M, it holds that in fact $u = 1$. Thus we can write:

$$SU(2) = \left\{ \begin{bmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{bmatrix} : |\alpha|^2 + |\beta|^2 = 1 \right\}$$

Hence $SU(2)$ is a three-dimensional sphere in $\mathbb{R}^4$.

As usual, complex matrices are much nicer than their real counterpart.

Theorem 16. *Every $A \in M_n(\mathbb{C})$ is unitarily upper-triagularizable.*

Proof. We wish to find unitary J so that $J^{-1}AJ$ is upper-triangular. The proof method will be by induction on size (or dimension), of which the case $n = 1$ is obvious.

To prove this, we want to find some J so that:

$$J^{-1}AJ = \begin{bmatrix} B & * \\ \mathbf{0} & A_1 \end{bmatrix}$$

where B is 1×1. At this point, we could use induction on A_1 to find J_1 so that $J_1^{-1}A_1J_1$ is upper-triangular, and then observe that:

$$(J(1 \oplus J_1))^{-1}AJ(1 \oplus J_1)$$

is upper-triagular and similar to A (where $J(1 \oplus J_1)$) is unitary).

So it suffices to find J. To find it, observe that the first column of J must be an eigenvector for A, with eigenvalue B. By the Fundamental Theorem of Algebra, χ_A has a complex root λ, which is an eigenvalue of A. Normalize an according eigenvector $\mathbf{v}_1$, then apply Gram-Schmidt to extend $\mathbf{v}_1$ to an orthogonal basis of $\mathbb{C}^n$, then normalize to extend an orthonormal basis. Letting:

$$J = \begin{bmatrix} \mathbf{v}_1 & \dots & \mathbf{v}_n \end{bmatrix}$$

And indeed, for this J:

$$J^{-1}AJ = \begin{bmatrix} \lambda & * \\ \mathbf{0} & * \end{bmatrix}$$

which completes the proof.

□

This is a pretty useful tool to have. However, unitaricity and Hermitianicity are strong conditions. We can strengthen the notion (or weaken the requirements, depending on your perspective) by considering **normal** matrices A, which satisfy $AA^* = A^*A$ (observe both classes of Hermitian and unitary matrices are a subclass of the normal matrices). It is an easy consequence of the definitions that:

Lemma 6. *Any matrix which is unitarily similar to a normal matrix is normal.*

In fact:

Lemma 7. *Every normal upper-triangular matrix is diagonal.*

Proof. We compare the iith entry of AA^* and A^*A. Observe that:

$$(AA^*)_{ii} = \sum_{j=i}^{n} |a_{2j}|^2$$

and

$$(A^*A)_{ii} = |a_{ii}|^2$$

Since these values are equal, it holds that $A_{ij} = 0$ if $j > i$. □

Together the Theorem and these two lemmas give:

Theorem 17. *Every normal matrix is unitarily diagonalizable.*

Which is extremely nice. In fact, this is a characterization! Every unitarily diagonalizable matrix is normal.

Theorem 18. *Suppose A is Hermitian. Then it is unitarily diagonalizable, with real diagonal entries.*

Proof. Since A is normal, it is unitarily similar to diagonal B. Hermitianicity is invariant under unitary similarity transforms, so $B = B^*$, hence $b_{ii} = \overline{b_{ii}}$ for all $i \in [n]$. □

Again, this is a characterization! It goes backwards easily; the forward direction was the tricky part.

We get an analogous result for unitary matrices:

Theorem 19. *Every unitary matrix is unitarily diagonalizable, with length 1 diagonal entries*

Proof. Let A be unitary; hence A is normal. If there is J unitary so that $J^{-1}AJ = B$ diagonal, by unitaricity it holds that $B^{-1} = J^{-1}AJ$, hence for all i, $b_{ii}^{-1} = \overline{b_{ii}}$, hence $|b_{ii}| = 1$. □

Again, the backwards direction is easy, so this is a characterization. This is the end of the nice nice results; we've taken our vacation in $\mathbb{C}$, but it's time to return to the drudgery of $\mathbb{R}$.

It is decidedly not the case that every real matrix is orthogonally upper-triangularizable. However, we do get a partial result:

Theorem 20. *Every symmetric real matrix A is orthogonally diagonlizable.*

Proof. Such a matrix A is Hermitian, so we know it is unitarily diagonalizable to a diagonal matrix B with real entries. We will not be using the unitary similarity, as it may involve complex coefficients. Instead, we observe that each eigenspace associated to an eigenvalue b_{ii} has geometric multiplicity equal to its algebraic multiplicity in χ_A, hence we can write $\mathbb{C}^n$ as an internal direct sum of (non-generalized!) eigenspaces. Even better, each of these eigenspaces are pairwise orthogonal (this follows from symmetry of A), so we simply compute an orthogonal basis for each, and concatenate them to obtain our real orthogonal similarity matrix. □

3.5 2/21/22: Back to Representation Theory

Armed with some complex linear algebra, we can now say nice sentences like:

Theorem 21. *Suppose $\mathscr{R} : G \to U_n(\mathbb{C})$ is a unitary representation of a group G. If $\mathscr{R}$ is reducible, then it is decomposable.*

The proof of this is short, but uses a tool which we know, but may not be theoretically intimate with:

Lemma 8. *Suppose $W \subseteq V$ is a subspace of a finite-dimensional inner product space. Then there exists a W-complementary subspace $W^\perp$ so that $W^{\perp\perp} = W$.*

Proof. We define:

$$W^\perp = \{\mathbf{x} \in V : \forall \mathbf{y} \in W, \langle \mathbf{y}, \mathbf{x} \rangle = 0\}$$

Indeed, $W^\perp$ is a subspace due to $\langle -, - \rangle$'s linearity in the second component; for all $\mathbf{x}, \mathbf{x}' \in V$ and $\lambda \in \mathbf{K}$:

$$0 = \langle \mathbf{y}, \mathbf{x} + \lambda \mathbf{x}' \rangle = \langle \mathbf{y}, \mathbf{x} \rangle + \lambda \langle \mathbf{y}, \mathbf{x}' \rangle = 0 + 0$$

so $\mathbf{x}, \mathbf{x}'$, and $\lambda \mathbf{x}' \in W^\perp$. To see that $W, W^\perp$ are complementary, first let $\mathbf{x} \in W \cap W^\perp$. Then $\langle \mathbf{x}, \mathbf{x} \rangle = 0$, so by positive-semidefiniteness $\mathbf{x} = \mathbf{0}$.

Now we need to show that $W \oplus W^\perp = V$. Indeed, we get for free the forward inclusion, so let $\mathbf{v} \in V$. Then it a classical theorem of linear algebra that we can write:

$$\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2$$

where $\mathbf{v}_1 \in W$, and $\mathbf{v}_2 \in W^\perp$. The method by which we arrive at this expression is via orthogonal projection. Let $\mathscr{B}$ be an orthonormal basis for W, and then let:

$$\mathbf{v}_1 = \sum_{\mathbf{b} \in \mathscr{B}} \frac{\langle \mathbf{b}, \mathbf{v} \rangle}{\langle \mathbf{b}, \mathbf{b} \rangle} \mathbf{b}$$

Evidently $\mathbf{v}_1 \in W$. Then if $\mathbf{v}_2 = \mathbf{v} - \mathbf{v}_1$, we see that $\mathbf{v}_2 \in W^\perp$, completing the decomposition. Hence W and $W^\perp$ are complementary.

To see that $W^{\perp\perp} = W$, we can just use some dimension counting. It is not hard to see that generally $W \subseteq W^{\perp\perp}$, and to see the reverse, observe that since $\mathbb{K}$ is a field, we can treat $\langle -, - \rangle$ as a dot product on a given basis. Under that basis, we can construct a matrix M so that $W^\perp = \text{null}(M^*)$, so rank-nullity gives that $\dim(W) = \dim(W^{\perp\perp})$. □

The orthogonal complement makes the proof of Theorem 21 easy.

Proof. Suppose $\mathbb{R}$ is a reducible unitary representation of G. Then there is some W so that W is G-invariant. We claim that $W^\perp$ is also G-invariant. Indeed, let $\mathbf{x} \in W^\perp$, $\mathbf{y} \in W$, and $g \in G$. Then:

$$\mathbf{y}^* f(g)\mathbf{x} = \mathbf{y}^* f(g)^* \mathbf{x} = (f(g)\mathbf{y})^* \mathbf{x} = 0$$

since $f(g)\mathbf{y} \in W$. Thus $f(g)\mathbf{x} \in W^\perp$, hence $\mathscr{R}$ is decomposable as the direct sum of $\mathscr{R}|_W$ and $\mathscr{R}|_{W^\perp}$. □

We can get a second proof of Maschke's Theorem, and perhaps a better sense of "what is going on," using the following:

Theorem 22. *Suppose G is finite and $\mathscr{R} : G \to GL_n(\mathbb{C})$ is a representation. Then $\mathscr{R}$ is isomorphic to a unitary representation $\mathscr{R}'$.*

Proof. Choose an arbitrary positive-definite Hermitian form F_A on $\mathbb{C}^n$. We claim that:

$$H = \sum_{g \in G} \mathscr{R}(g)^* A \mathscr{R}(g)$$

is Hermitian positive-definite and invariant under conjugate-transpose similarity by $\mathscr{R}(g)$. Indeed, H is a sum of Hermitian positive-definite matrices, hence it is Hermitian positive-definite itself. To see invariance:

$$\mathscr{R}(h)^* H \mathscr{R}(h) = \sum_{g \in G} \mathscr{R}(gh)^* A \mathscr{R}(gh) = \sum_{g' \in G} \mathscr{R}(g')^* A \mathscr{R}(g')$$

Since H defines an inner product with respect to a basis J, it holds that $J^* H J = I$. In other words, $H = (J^*)^{-1} J^{-1}$, thus:

$$\mathscr{R}(g)^* (J^*)^{-1} J^{-1} \mathscr{R}(g) = \mathscr{R}(g)^* H \mathscr{R}(g) = H = (J^*)^{-1} J^{-1}$$

since H is invariant under conjugate-transpose similarity by $\mathscr{R}(g)$. Clearing the right-hand side:

$$(J^* \mathscr{R}(g)^* (J^{-1})^*)(J^{-1} \mathscr{R}(g) J) = I$$

So $J^{-1}\mathscr{R}(g)J$ is unitary. Observing that J is uniform across $g \in G$, this gives an isomorphism of representations $\mathscr{R} \to \mathscr{R}'$, where $\mathscr{R}' = J^{-1}\mathscr{R}J$ is unitary. □

Corollary 6 (Maschke's Theorem, Redux)**.** *Every reducible representation of a finite group is decomposable.*

Proof. Suppose $\mathscr{R}$ is a representation of a finite group. Then it is isomorphic to a unitary representation $\mathscr{R}'$ by Theorem 22, and by Theorem 21, reducibility of $\mathscr{R}'$ implies decomposability of $\mathscr{R}'$, hence $\mathscr{R}$. □

Together Theorems 21 and 22 gives a proof of Theorem 10, which was "obvious" but not at all clear to prove:

Theorem 23 (Theorem 10, Redux)**.** *Every representation of a finite group G is equivalent to a direct sum of irreducible representations.*

Proof. This follows from Maschke's Theorem and induction on the dimension of the representation. If $\mathscr{R}$ is not irreducible, we can reduce it into a direct sum of at least two lesser-dimension representations. Induction completes the proof. □

Stricter requirements on G can produce remarkably strict representations:

Theorem 24. *Every irreducible finite-dimensional representation of an abelian group G over $\mathbb{C}$ is 1-dimensional.*

Proof. Suppose that $\mathscr{R} : G \to GL_n(\mathbb{C})$ is a representation, where G is abelian and $\mathscr{R}$ is irreducible. We wish to show that $n = 1$.

For any $g \in G$, let λ be an eigenvalue of $\mathscr{R}(g)$. Then $W = \ker(\mathscr{R}(g) - \lambda I) \neq \{\mathbf{0}\}$. Next we will use the trick that "commmuting operators preserve eigenspaces." Let $h \in G$ and $\mathbf{x} \in W$:

$$\begin{aligned}(\mathscr{R}(g) - \lambda I)\mathscr{R}(h)\mathbf{x} &= \mathscr{R}(g)\mathscr{R}(h)\mathbf{x} - \lambda\mathscr{R}(h)\mathbf{x} \\ &= \mathscr{R}(h)\mathscr{R}(g)\mathbf{x} - \mathscr{R}(h)\lambda\mathbf{x} \\ &= \mathscr{R}(h)(\mathscr{R}(g)\mathbf{x} - \lambda\mathbf{x}) \\ &= \mathbf{0}\end{aligned}$$

Thus $\mathscr{R}(h)\mathbf{x} \in W$, so W is a G-invariant subspace. Because $\mathscr{R}$ is irreducible, $W = \mathbb{C}^n$, hence $\mathscr{R}(g) = \lambda I$.

This implies that $n = 1$. After all, every representation of $g \in G$ is diagonal, so $\mathbb{C}\mathbf{e}_1$ is a nontrivial G-invariant subspace if and only if $n > 1$, hence $\mathscr{R}$ is reducible if and only if $n > 1$. □

Thus a great many representations go into $\mathbb{C}$, and they have quite an interesting structure. Here we will coarsely discuss the notions we are to delve into.

Suppose that $g \in G$ and $\mathscr{R} : G \to \mathbb{C}$ is a representation. If $|G| = k$, it holds that $g^k = e$, so $\mathscr{R}(g)^k = 1$, thus $\mathscr{R}(g)$ is an lth root of unity, where l divides k.

We will be discussing a notion we will call the "character" of a group. First we will think of a special case. A **character** of a finite abelian group is any group homomorphism $\chi : G \to \mathbb{C}$. If we fix G, we get a group $\widehat{G}$ of characters of G under pointwise multiplication.

For example, take $\mathbb{Z}/n\mathbb{Z}$. The character is uniquely determined by where it sends $[1]$, so we may identify $\widehat{\mathbb{Z}/n\mathbb{Z}}$ with the set $M_n = \{\mu \in \mathbb{C} : \mu^n = 1\}$; in fact, this is a group isomorphism! However, the homomorphism is noncanonical; we may send the generator $[1]$ to any generator of the same order in M_n.

That said, we can obtain a pleasant duality by observing there is a unique isomorphism $\widehat{\widehat{G}} \cong G$.

It is a surprising turn of events that the generalization of a character to non-abelian groups looks very different. Suppose that G is any finite group, and $\mathscr{R} : G \to GL_n(\mathbb{C})$ is any representation. Then the **character** of $\mathscr{R}$ is the function:

$$\text{trace}(\mathscr{R}(g)) : G \to \mathbb{C}$$

A surprising fact about the character (that we get for free in the abelian case) is that it is invariant under group conjugation.

Lemma 9. *For all $g, h \in G$:*

$$\text{trace}(\mathscr{R}(h^{-1}gh)) = \text{trace}(\mathscr{R}(g))$$

Proof. This follows from the fact that trace is invariant under cyclic shift, and that $\mathscr{R}$ is a homomorphism. □

3.6 2/25/22: The Character of a Representation

Suppose that $\mathscr{R} : G \to GL_n(\mathbb{C})$ is a representation. We define the **character** of $\mathscr{R}$ to be the function $\chi_{\mathscr{R}} : G \to \mathbb{C} \setminus \{0\}$:

$$\chi_{\mathscr{R}}(g) = \text{trace}(\mathscr{R}(g))$$

To give an idea of where we are going, we want to build up the useful algebraic sidearm known as:

Theorem 25 (Schur Orthogonality Relations)**.** *Suppose $|G| < \infty$, and $\mathscr{R}_1, \mathscr{R}_2$ irreducible representations of G. Then if χ_1 and χ_2 are their characters:*

$$\frac{1}{|G|} \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)} = \begin{cases} 1 & \text{if } \mathscr{R}_1 \cong \mathscr{R}_2 \\ 0 & \text{otherwise} \end{cases}$$

It may seem like the conjugation comes out of nowhere, but it turns out that conjugation of the character is precisely inversion of the input:

Lemma 10. *Suppose χ is the character of any representation $\mathscr{R}$ of G, and $|G| < \infty$. Then for every $g \in G$:*

$$\chi(g^{-1}) = \overline{\chi(g)}$$

At this point, we've developed a good deal of machinery, so we can provide two proofs, each of a different flavor. The first proof uses unitaricity:

Proof. Since G is finite, there is some $J \in GL_n(\mathbb{C})$ such that $J^{-1}\mathscr{R}J$ is unitary.

Observe that in such a representation:

$$J^{-1}\mathscr{R}(g)^{-1}J = (J^{-1}\mathscr{R}(g)J)^{-1} = (J^{-1}\mathscr{R}(g)J)^*$$

Thus:

$$\begin{aligned}
\chi(g^{-1}) &= \text{trace}(\mathscr{R}(g^{-1})) \\
&= \text{trace}(J^{-1}\mathscr{R}(g)^{-1}J) && \text{(by class function)} \\
&= \text{trace}((J^{-1}\mathscr{R}(g)J)^*) && \text{(by unitaricity)} \\
&= \overline{\text{trace}(J^{-1}\mathscr{R}(g)J)} && \text{(by definition of the conjugate transpose)} \\
&= \overline{\text{trace}(\mathscr{R}(g))} && \text{(by class function (again!))} \\
&= \overline{\chi(g)}
\end{aligned}$$

□

The second proof uses the Jordan canonical form:

Proof. Since $|G| < \infty$, each $g \in G$ has finite order. If $k = \text{ord}(g)$, then $\mathscr{R}(g)^k = I$, so if J is a Jordan basis of $\mathscr{R}(g)$ and C its Jordan canonical form:

$$C^k = (J^{-1}\mathscr{R}(g)J)^k = J^{-1}\mathscr{R}(g)^k J = I$$

hence C is diagonal, with diagonal entries c_{ii} that satisfy $c_{ii}^k = 1$. As is well-known, the c_{ii} are the eigenvalues of $\mathscr{R}(g)$. Thus for any eigenvalue λ of $\mathscr{R}(g)$, $\lambda^k = 1$, so $|\lambda|^k = 1$, hence $|\lambda| = 1$. Since $\lambda\overline{\lambda} = |\lambda|^2 = 1$, it follows that $\overline{\lambda} = \lambda^{-1}$.

Hence:

$$\begin{aligned}
\chi(g^{-1}) &= \text{trace}(\mathscr{R}(g)^{-1}) \\
&= \sum_{i=1}^{n} \lambda_i^{-1} && \text{(since eigenvalues of inverse are inverse of eigenvalues)} \\
&= \sum_{i=1}^{n} \overline{\lambda_i} && \text{(by the reasoning above)} \\
&= \overline{\sum_{i=1}^{n} \lambda_i} && \text{(by additivity of the complex conjugate)} \\
&= \overline{\text{trace}(\mathscr{R}(g))} \\
&= \overline{\chi(g)}
\end{aligned}$$

□

Next up on the royal road to Schur's Orthogonality Relations is Schur's Lemma:

Lemma 11 (Schur)**.** *Let $|G| < \infty$. Further suppose that $\mathscr{R}_1$ and $\mathscr{R}_2$ are n_1 and n_2-dimensional irreducible representations of G. Moreover, suppose that $L : \mathbb{C}^{n_1} \to \mathbb{C}^{n_2}$ is linear such that:*

$$L \circ \mathscr{R}_1 = \mathscr{R}_2 \circ L$$

Then:

1. *If $\mathscr{R}_1 \ncong \mathscr{R}_2$, it must be that $L = \mathbf{0}$.*
2. *If $\mathscr{R}_1 = \mathscr{R}_2$ then $L = \lambda I$ for some λ.*

Proof. The first part of the proof follows from the fact that commuting linear operators "preserve special subspaces;" in this case, it is the kernel and image.

We will assume that $L \neq \varnothing$, and show that L is a bijection. Thus L will be a certificate that $\mathscr{R}_1 \cong \mathscr{R}_2$, which is precisely the contrapositive of (1).

First, we claim that $\ker(L)$ is $\mathscr{R}_1(G)$-invariant. Indeed, Suppose that $g \in G$, and let $\mathbf{x} \in \ker(L)$. Then $L\mathbf{x} = \mathbf{0}$, and to see that $\mathscr{R}_1(g)\mathbf{x} \in \ker(L)$:

$$L\mathscr{R}_1(g)\mathbf{x} = \mathscr{R}_2(g)L\mathbf{x} = \mathscr{R}_2(g)\mathbf{0} = \mathbf{0}$$

Hence $\mathscr{R}_1(G)(\ker(L)) \subseteq \ker(L)$, thus by $\mathscr{R}_1$'s irreducibility, $\ker(L)$ is either $\mathbf{0}$ or $\mathbb{C}^{n_1}$. Since $L \neq \mathbf{0}$, it cannot be $\mathbb{C}^{n_1}$, so L is injective.

On the other hand, we will show that $\mathrm{im}(L)$ is $\mathscr{R}_2(G)$-invariant in $\mathbb{C}^{n_2}$. Suppose that $\mathbf{y} \in \mathrm{im}(L)$. Then:

$$\mathscr{R}_2(g)\mathbf{y} = \mathscr{R}_2(g)L\mathbf{x} = L\mathscr{R}_1(g)\mathbf{x}$$

so $\mathscr{R}_2(g)\mathbf{y} \in \mathrm{im}(L)$, and by irreducibility, $\mathrm{im}(L)$ is either $\mathbf{0}$ or $\mathbb{C}^{n_2}$. Since $L \neq \mathbf{0}$, it is not $\mathbf{0}$, hence L is surjective.

Therefore L is a bijection, and hence a certificate of isomorphism.

To see the second part of Schur's Lemma, the aforementioned "special subspaces" are eigenspaces.

Suppose $\mathscr{R} : G \to GL_n(\mathbb{C})$ is a representation, and let L be linear so that $L\mathscr{R} = \mathscr{R}L$. For all λ eigenvalues of L, write:

$$V_\lambda = \ker(L - \lambda I)$$

Then for every $g \in G$ and $\mathbf{x} \in V_\lambda$, it holds that $\mathscr{R}(g)\mathbf{x} \in V_\lambda$ (since λI is in $GL_n(\mathbb{C})$'s center)

$$(L - \lambda I)\mathscr{R}(g)\mathbf{x} = \mathscr{R}(g)(L - \lambda I)\mathbf{x} = \mathscr{R}(g)\mathbf{0} = \mathbf{0}$$

hence V_λ is $\mathscr{R}(G)$-invariant. Since λ is an eigenvalue, $V_\lambda \neq \{\mathbf{0}\}$, so by irreducibility $V_\lambda = \mathbb{C}^n$. Thus for every $\mathbf{x} \in \mathbb{C}^n$, $L\mathbf{x} = \lambda\mathbf{x}$, which is to say that $L = \lambda I$.

□

The second part of Schur's Lemma is rather interesting when we consider:

Lemma 12.

$$Z(GL_n(\mathbb{C})) = \left\{ \begin{bmatrix} \lambda & & \\ & \ddots & \\ & & \lambda \end{bmatrix} : \lambda \neq 0 \right\}$$

Proof. Evidently all constant-diagonal matrices are in $GL_n(\mathbb{C})$'s center; on the other hand, let M_{ii} be the iith basis vector in $M_n(\mathbb{C})$'s standard basis.

Letting $X \in Z(GL_n(\mathbb{C}))$, it holds that:

$$\sum_{q=1}^{n} (M_{ii})_{lq} X_{qk} = (M_{ii}X)_{lk} = (XM_{ii})_{lk} = \sum_{p=1}^{n} X_{lp}(M_{ii})_{pk}$$

For each $i \in [n]$. However, since $(M_{ii})_{lq} = 1$ if $q = l = i$ and 0 elsewise, and $(M_{ii})_{pk} = 1$ if $p = k = i$ and 0 elsewhere, it follows that X is diagonal.

In order for X to commute with the all-ones matrix, it must be constant-diagonal, completing the proof.

□

However, if we want to nuke the lemma, here is an alternative proof:

Proof. Evidently $\lambda I \in Z(GL_n(\mathbb{C}))$. Suppose that $X \in Z(GL_n(\mathbb{C}))$. Then X commutes with every matrix; in particular, it commutes with any irreducible representation, hence $X = \lambda I$ for some $\lambda \neq 0$. □

Thus part 2 of Schur's Lemma can be thought of describing how irreducible representations give the "worst case" for possible commutators.

In our journey to Schur's orthogonality relations, we will abstract away to a larger class of representations, and observe that their characters depend in exactly the right way on simpler representations.

Indeed, if $|G| < \infty$ and $\mathscr{R}_1$ and $\mathscr{R}_2$ are representations of G, then the set of **intertwiners of $\mathscr{R}_1$ and $\mathscr{R}_2$**:

$$\{L : \mathbb{C}^{n_1} \to \mathbb{C}^{n_2} : L\mathscr{R}_1 = \mathscr{R}_2 L\}$$

is a $\mathbb{C}$-vector subspace of $\hom(\mathbb{C}^{n_1}, \mathbb{C}^{n_2})$. Due to this, we will denote the set of intertwiners as $\hom(\mathscr{R}_1, \mathscr{R}_2)$.

An act of translation yields:

Corollary 7 (Schur's Lemma)**.** *: If $|G| < \infty$, and $\mathscr{R}_1$ and $\mathscr{R}_2$ are irreducible representations of G, then:*

$$\dim \hom(\mathscr{R}_1, \mathscr{R}_2) = \begin{cases} 1 & \text{if } \mathscr{R}_1 \cong \mathscr{R}_2 \\ 0 & \text{else} \end{cases}$$

To prove Schur's orthogonality relations, it thus amounts to showing:

$$\dim \hom(\mathscr{R}_1, \mathscr{R}_2) = \frac{1}{|G|} \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)}$$

To prove the next lemma, we define for $|G| < \infty$ and $\mathscr{R} : G \to GL(V)$, the fixed-point-set of $\mathscr{R}(G)$:

$$V^{\mathscr{R}(G)} = \{\mathbf{x} \in V : \mathscr{R}(g)\mathbf{x} = \mathbf{x}, \forall g \in G\}$$

This is clearly $\mathscr{R}(G)$-invariant. Moreover, this set is "fundamental" in the following fashion: every representation of G is a direct sum of finite-dimensional irreducible representations, and one of these irreducible representations will be the one-dimensional representation $g \mapsto \begin{bmatrix}1\end{bmatrix}$ for all $g \in G$.

For example, if we let S_n act on $\mathbb{C}^n$ by permutation of coordinates; i.e., each $\sigma \in S_n$ represented by the corresponding permutation matrix M^σ; then $(\mathbb{C}^n)^{\mathscr{R}(S_n)}$ is $\mathbb{C}\mathbf{1}$. Up to a change of basis sending $\mathscr{R}$ to $\mathscr{R}'$, this line is sent to $\mathbb{C}\mathbf{e}_1$, in which case the matrix representations will all be of the form $\begin{bmatrix}1\end{bmatrix} \oplus \mathscr{R}'(g)_{\{2,\ldots,n\}}$.

[Note: The proof of the following lemma seems off. It's not cohering in my head, but I can't quite tell what's wrong with it. It's not a huge deal, since it's not relevant to the larger class of theory, but I'd like to make a note of this.]

Lemma 13. *Suppose $|G| < \infty$ and $\mathscr{R}$ a representation of G. Then:*

$$\dim V^{\mathscr{R}(G)} = \text{trace}\left(\frac{1}{|G|}\sum_{g\in G}\mathscr{R}(g)\right) = \frac{1}{|G|}\sum_{g\in G}\chi(g)$$

This is getting closer to what we want. Indeed, $V^{\mathscr{R}(G)} = \hom(\mathscr{R}_1, \mathscr{R})$, where $\mathscr{R}_1$ is the trivial representation, so this is a special case of the general orthogonality relations, and will be used to prove the general case.

Proof. First we show that this is true when $\mathscr{R}$ is irreducible. To see this, define:

$$L = \frac{1}{|G|}\sum_{g\in G}\mathscr{R}(g)$$

By construction, L is an intertwiner of $\mathscr{R}$ with itself, so by Schur's Lemma $L = \lambda I$ for $\lambda \neq 0$. To find λ, we observe:

$$L^2 = \frac{1}{|G|^2}\sum_{g,h\in G}\mathscr{R}(gh) = \frac{1}{|G|^2}\sum_{g\in G}|G|\mathscr{R}(g) = L$$

Since $L = \lambda I$, it follows that $\lambda^2 = \lambda$, hence $\lambda \in \{0, 1\}$. Since $\lambda \neq 0$, it follows that $\lambda = 1$. Then:

$$\frac{1}{|G|}\sum_{g\in G} n = n$$

To conclude this case, observe that $n = \dim V^{\mathscr{R}(G)}$.

To see the general case of a reducible finite group representation, observe that both the dimension and character are linear in the direct sum.

□

Next section is Schur's orthogonality relations.

3.7 2/28/22: Schur's Orthogonality Relations and the Space of Characters

To prove Theorem 25, we will utilize the following important construction. Suppose that $\mathscr{R}_1 : G \to GL_{n_1}(\mathbb{C})$ and $\mathscr{R}_2 : G \to GL_{n_2}(\mathbb{C})$ are two representations. Then we can define a new representation:

$$\mathscr{R}^{\text{hom}} : G \to \hom(\mathbb{C}^{n_1}, \mathbb{C}^{n_2})$$

with the given rule:

$$\mathscr{R}^{\text{hom}}(g)L = \mathscr{R}_2(g)L\mathscr{R}_1(g)^{-1}$$

The proof verifying that this is a homomorphism, and hence a representation, is essentially the same proof that the conjugation action is indeed an action, and we omit it.

The interesting part about this map relates to intertwiners. Indeed, L intertwines $\mathscr{R}_1$ and $\mathscr{R}_2$ if and only if $\mathscr{R}^{\text{hom}}L = L$, so understanding the structure of $\mathscr{R}^{\text{hom}}$ is both necessary and sufficient to understand intertwiners.

In fact, in the language of last section:

$$\hom(\mathbb{C}^{n_1}, \mathbb{C}^{n_2})^{\mathscr{R}^{\text{hom}}} = \hom(\mathscr{R}_1, \mathscr{R}_2)$$

Thus using Lemma 13 and Schur's Lemma, if $\chi_{\text{hom}}(g)$ is the character of $\mathscr{R}^{\text{hom}}(g)$:

$$\frac{1}{|G|}\sum_{g\in G}\chi_{\text{hom}}(g) = \dim \hom(\mathbb{C}^{n_1}, \mathbb{C}^{n_2})^{\mathscr{R}^{\text{hom}}} = \begin{cases} 1 & \text{if } \mathscr{R}_1 \cong \mathscr{R}_2 \\ 0 & \text{else} \end{cases}$$

To finish the proof of Schur's orthogonality relations, we need only show:

Lemma 14.

$$\chi_{\text{hom}}(g) = \chi_2(g)\chi_1(g^{-1})$$

Proof. This is not a hard proof in detail, but it is tricky in abstraction– the key is to think about a linear map as a vector. In particular, we wish to compute the trace of the map sending:

$$L \mapsto \mathscr{R}_2(g)L\mathscr{R}_1(g)^{-1}$$

This is a map $Q : \mathbb{C}^{n_2\times n_1} \to \mathbb{C}^{n_2\times n_1}$, and is linear in this space.

Thus to compute the trace, it amounts to considering the map's action on the basis $\{\mathbf{e}_i\mathbf{e}_j^t\}_{i\in[n_2],j\in[n_1]}$, and summing the respective entries of the action on each basis element. If we consider the general map $L \mapsto ALB$:

$$
\begin{aligned}
\operatorname{trace}(Q) &= \sum_{i,j} (Q(\mathbf{e}_i \mathbf{e}_j^t))_{ij} \\
&= \sum_{i,j} (A\mathbf{e}_i \mathbf{e}_j^t B)_{ij} \\
&= \sum_{i,j} ((A\mathbf{e}_i)(\mathbf{e}_j^t B))_{ij} \\
&= \sum_{i,j} (\operatorname{col}_i(A)_j(B))_{ij} \\
&= \sum_{i,j} A_{ii} B_{jj} && \text{(by definition of matrix multiplication)} \\
&= \sum_i A_{ii} \sum_J B_j j \\
&= \operatorname{trace}(A)\operatorname{trace}(B)
\end{aligned}
$$

Which finishes the proof. □

Thus we have a complete proof of Schur's orthogonality relations:

Proof.

$$
\begin{aligned}
\frac{1}{|G|} \sum_{g \in G} \chi_2(g) \overline{\chi_1(g)} &= \frac{1}{|G|} \sum_{g \in G} \chi_{\hom}(g) && \text{(by Lemma 14)} \\
&= \dim \hom(\mathbb{C}^{n_1}, \mathbb{C}^{n_2})^{\mathscr{R}^{\hom}} && \text{(by Lemma 13)} \\
&= \begin{cases} 1 & \text{if } \mathscr{R}_1 \cong \mathscr{R}_2 \\ 0 & \text{else} \end{cases} && \text{(by Schur's Lemma)}
\end{aligned}
$$

□

Schur's orthogonality relations give us a fair bit more meat than is immediately obvious. For any group G, we can define the **complex group ring** $\mathbb{C}[G]$, which is the set of formal sums:

$$
\left\{ \sum_{i=1}^{n} \lambda_i g_i : \lambda_i \in \mathbb{C}, g_i \in G, n \in \mathbb{N} \right\}
$$

where addition collects over the g_i, and multiplication acts as $\cdot$ on $\mathbb{C}$, and $*$ on G.

This is a vector space of dimension $|G|$, and has an interesting relationship with another vector space. We say that a function $G \to \mathbb{C}$ is a **class function** if it is constant on G's conjugacy classes. In particular, we have observed that characters of G are class functions.

The space of class functions of G, which we will write as class(G), is in fact a vector space in its own right, of dimension $|\{\text{conjugacy classes of } G\}|$. There is a nice correspondence between class(G) and $\mathbb{C}[G]$; observe that $Z(\mathbb{C}[G])$ is a vector subspace of $\mathbb{C}[G]$. We claim that there is a linear isomorphism between class(G) and $Z(\mathbb{C}[G])$.

Indeed, define $I : \text{class}(G) \to Z(\mathbb{C}[G])$ by the rule:

$$\tau \mapsto \sum_{g \in G} \tau(g) g$$

I is clearly injective and linear; is it bijective, and does it actually fall into the codomain? To see that I doesn't send class(G) outside the codomain, and hits every element of the codomain:

Lemma 15. *Let $\tau : G \to \mathbb{C}$. Then τ is class if and only if $I(\tau) \in Z(\mathbb{C}[G])$.*

Proof. Since $\mathbb{C}$ is commutative, $\alpha := I(\tau) \in Z(\mathbb{C}[G])$ if and only if $\alpha h = h\alpha$ for each $h \in G$. What are these expressions? Observing that for each $g' \in G$, $hg = g'$ if and only if $h^{-1}g' = g$, the α commutes with h if and only if:

$$\sum_{g' \in G} \tau(h^{-1}g')g' = \sum_{g' \in G} \tau(g'h^{-1})g'$$

Thus α commutes with h if and only if $\tau(hg) = \tau(gh)$ for every $g, h \in G$. However, this is precisely what it means to be a class function!

Suppose that τ is class. Then $\tau(hg) = \tau(h^{-1}hgh) = \tau(gh)$. To see the converse, if $\tau(gh) = \tau(hg)$ for every $g, h \in G$, then:

$$\tau(g_1 g_2 g_1^{-1}) = \tau(g_1(g_2 g_1^{-1})) = \tau((g_2 g_1^{-1})g_1) = \tau(g_2)$$

Thus α commutes with h if and only if τ is a class function. □

This vector subspace is well-behaved enough that it has a nice sesquilinear form; one can phrase the following in terms of $Z(\mathbb{C}[G])$, but with the existing theory it is easier to think of $Z(\mathbb{C}[G])$ as class(G). Thus we may equip class(G) with the sesquilinear form:

$$\langle \tau_1, \tau_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \tau_1(g)\overline{\tau_2(g)}$$

Look familiar? Our next project is to leverage Schur's orthogonality relations for the following beautiful result:

Theorem 26. *Suppose $|G| < \infty$. The characters of distinct irreducible representations of G form an orthogonal basis of* class(G).

Which, among many things, tells us:

Corollary 8. *The number of distinct irreducible representations of G is the same as the number of conjugacy classes of G.*

Proving Theorem 26 uses quite a few nice tricks.

Proof. Let $X = \{\chi_1, \ldots, \chi_k\}$ be a set of distinct irreducible characters of G. Immediate from the orthogonality relations is that X is orthogonal. We need to show it spanning and linearly independent. The latter follows from orthogonality; if:

$$\sum_{i=1}^{k} c_i \chi_i = 0$$

then for each j:

$$0 = \langle 0, \chi_j \rangle = \left\langle \sum_{i=1}^{k} c_i \chi_i, \chi_j \right\rangle = \sum_{i=1}^{k} c_i \langle \chi_i, \chi_j \rangle = c_j$$

Thus $c_j = 0$.

To show X spans class(G), it amounts to showing that if $\langle \tau, \chi_j \rangle = 0$ for every $j \in [k]$, then $\tau = 0$. That is to say, $X^\perp = \{0\}$, so $X = \text{class}(G)$ (here we implicitly use that G is finite, hence $\dim \text{class}(G)$ is finite).

The following trick is quite nice. Something special about the complex group ring is that it bridges actions and representations; in particular, we can extend any action on G to a representation on $\mathbb{C}[G]$, so why not the regular action? Define the **regular representation** of G by the map $\mathscr{R} : G \to \mathbb{C}[G]$ with the rule:

$$g \cdot \sum_{g \in G} \lambda_g g \mapsto \sum_{g' \in G} \lambda_g g g'$$

Since $|G| < \infty$, $\mathscr{R}$ is isomorphic to a direct sum of irreducible representations.

Now suppose that $\langle \tau, \chi_j \rangle = 0$ for each $j \in [k]$. In particular, the characters of the blocks of the decomposition of $\mathscr{R}$ are irreducible characters in X, so $\langle \tau, \chi_{\mathscr{R}} \rangle = 0$.

It is not hard to show that if τ is any class function, and r any representation of G, that $L = \sum_{g \in G} \tau(g) r(g^{-1})$ is an intertwiner of r:

$$r(h) L r(h)^{-1} = \sum_{g \in G} \tau(g) r(hgh^{-1}) = \sum_{g \in G} \tau(hgh^{-1}) r(hgh^{-1}) = L$$

If r is irreducible, it follows that $L = \lambda I$ by Schur's Lemma. However:

$$\text{trace}(L) = \lambda n = \sum_{g \in G} \tau(g) \overline{\text{trace}(r(g))} = \sum_{g \in G} \tau(g) \overline{\chi(g)} = \langle \tau, \chi \rangle = 0$$

Thus if r is irreducible, $L = 0$. However, using linearity of decomposition, it holds that $L = 0$ if r is not, so for all representations of G the according L is 0.

In particular, this holds for the regular representation by our assumption of $\tau \perp X$. Thus $L\mathscr{R}(e) = 0$, but since $\mathscr{R}(e) = I$, it follows that:

$$\sum_{g \in G} \tau(g) g^{-1} = 0$$

hence $\tau(g) = 0$ for all g, which is what we wished to show.

□

Next up, modules!

Chapter 4

Elementary Module Theory

4.1 3/2/22: The Definition of a Module

Suppose that R has unity, but is not necessarily commutative. We say that a **left R-module**, or left module *over* R, is a triplet $(M, +, \cdot)$, where $+$ is a binary operation on M, and $\cdot : R \times M \to M$ so that:

1. $(M, +)$ is an abelian group,
2. for all $m \in M$, it is the case that $1 \cdot m = m$,
3. for all $r_1, r_2 \in R$, and all $m \in M$, it holds that $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$,
4. for all $r_1, r_2 \in R$, and all $m \in M$, it is true that $(r_1 + r_2) \cdot m = (r_1 \cdot m) + (r_2 \cdot m)$, and
5. for all $r \in R$, and all $m_1, m_2 \in M$, $r \cdot (m_1 + m_2) = (r \cdot m_1) + (r \cdot m_2)$.

Some basic corollaries are that $0_R \cdot m = 0_M$, and $(-r) \cdot m = -(r \cdot m)$. Here are some classical examples:

1. Every abelian group is a $\mathbb{Z}$-module, and vice-versa; define:

$$z \cdot m = \begin{cases} 0 & \text{if } n = 0 \\ \sum_{i=1}^{z} m & \text{if } n > 0 \\ \sum_{i=1}^{z} (-m) & \text{if } n < 0 \end{cases}$$

2. Every vector space V over a field K is a K-module.
3. We have already investigated a correspondence between complex representations of a group G, and left $\mathbb{C}[G]$-modules; given a $\mathbb{C}[G]$-module M, we can define for each $g \in G$ a function $\mathscr{R} : M \to M$ by the rule:

$$\mathscr{R}(g)m = g \cdot m$$

   for all $m \in M$. This evidently satisfies the rules of a representation.

   On the other hand, if $\mathscr{R} : G \to GL(V)$ is a represenation, we let $M = V$, and for every element $r = \sum_{i=1}^{n} c_i g_i \in \mathbb{C}[G]$, we let $r \cdot m = \sum_{i=1}^{n} c_i f(g_i)m$.
4. Any ring R is a left (or right) module over itself.

As with every algebraic object, we get a notion of homomorphism. However, as the coefficient ring R may vary over a given R-module M, we introduce one extra piece of information (which we conveniently omit when irrelevant). If R is a ring, and M_1 and M_2 are R-modules, we say that an **R-module homomorphism** is a function $f : M_1 \to M_2$ which satisfies:

1. $f(m_1 + m_2) = f(m_1) + f(m_2)$, and
2. $f(rm) = rf(m)$ (observe this hinges on both M_1 and M_2 being R-modules).

We also get a subobject; suppose that M is an R-module. An **R-submodule** of M is some $N \subseteq M$ so that:

1. $N + N \subseteq N$, and
2. $RN \subseteq N$

That is to say, an R-submodule of an R-module is a subset of that R-module which itself is an R-module. In general, the intersection of any collection of submodules is itself a submodule, but this obviously does not hold for unions. We instead get a partial result:

Lemma 16. *Suppose that M is an R-module, and*

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$$

is an increasing sequence of R-submodules of M. Then $\bigcup_{n\in\mathbb{N}} M_n$ is an R-submodule of M.

This is also not too hard to see.

The conditions for submodules look familiar– we have encountered before a subobject which is an additive subgroup that absorbs multiplication. We refer to an ideal, and in fact left (right) ideals are left (right) submodules of R as a left (right) R-module! In this sense, thinking of a ring R as an R-module may be more natural than just as a ring, as submodules are a more lax requirement than a subring.

We also get the canonical subobjects in this theory.

Theorem 27. *Suppose that $f : M_1 \to M_2$ is an R-module homomorphism. Then* $\mathrm{im}(f)$ *is an R-submodule of M_2.*

Proof. It is a subgroup since the image of a group homomorphism is a subgroup. To show the second condition, suppose that $y \in \mathrm{im}(f)$. Then we can write $y = f(x)$ for some $x \in M_1$. Then $ry = rf(x) = f(rx) \in \mathrm{im}(f)$. □

Compare this to the fact that $\mathrm{im}(g)$ is not necessarily an ideal of the image ring, if g is a ring homomorphism. We leave it as an exercise to ponder where the proof breaks, if we apply the same line of reasoning to g. This may make modules look like nicer objects, but in fact, the niceness of the proof only follows from the fact that this is a homomorphism of R-modules *in particular*. An analogous notion of homomorphism between modules over different rings will not work so well. However, the second canonical subobject is always nice:

Theorem 28. *If $f : M_1 \to M_2$ is an R-module homomorphism, then* $\ker(f)$ *is an R-submodule of M_1.*

This is the classic proof, and we omit it.

4.2 3/4/22: Basic Tools of Module Theory

[Here Borisov explains a broken proof from a previous lecture. Look to a friend if needed.]

Last time we stated the theory of modules over unital rings, but here on in, we will assume R is a CRU.

We have modules and submodules; are there quotient modules? There are, and in fact they are much better behaved than the quotienting subobjects of group and ring theory; we can *always* quotient by a submodule. In this sense, quotient modules are more akin to quotient vector spaces.

Suppose that M is an R-module and $N \subseteq M$ is an R-submodule. The **quotient** of M by N is the quotient of the corresponding abelian groups with the multiplication rule:

$$r[m] = [rm]$$

Is multiplication well-defined? Indeed, if $[m] = [m']$, then $m - m' \in N$, so $r(m-m') \in N$, hence $rm - rm' \in N$, which is just that $[rm] = [rm']$.

It is worth noting that quotient modules are not "strictly nicer" than other algebraic quotient objects, just because all submodules can quotient. Indeed, if we take the $\mathbb{Q}$-module $\mathbb{R}$, we know that $\mathbb{R}/\mathbb{Z}$ makes sense as a quotient group, but $\mathbb{Z}$ is not a $\mathbb{Q}$-submodule of $\mathbb{R}$, hence there is no sensible "quotient $\mathbb{Q}$-submodule $\mathbb{R}/\mathbb{Z}$." It is better to think of the construction as *different*, not strictly more flexible.

The next tool is a bit of clever language, which encodes a remarkable amount of structure. We say that a sequence of maps:

$$0 \to M_1 \xrightarrow{\pi} M \xrightarrow{\tau} M_2 \to 0$$

is a **short exact sequence of modules** if $M_2 \cong M/M_1$. By the first isomorphism theorem of modules, this is equivalent to the condition that induces the term "exact:" that $\mathrm{im}(\pi) = \ker(\tau)$. After all, if $M_1 \subseteq M$, the first isomorphism theorem is just the statement that the sequence:

$$0 \to M_1 \to M \to M/M_1 \to 0$$

is short exact.

In general, we say a sequence of maps:

$$\ldots \xrightarrow{f_n} Q_{n+1} \xrightarrow{f_{n+1}} Q_{n+2} \xrightarrow{f_{n+2}} \ldots$$

is **exact** if $\mathrm{im}(f_n) = \ker(f_{n+1})$. The above sequence is called short because... well, it's short.

Here is why this is a nice matter of language:

Lemma 17. *π is injective if and only if $0 \to M_1 \xrightarrow{\pi} M$ is exact.*

Lemma 18. *τ is surjective if and only if $M \xrightarrow{\tau} M_2 \to 0$ is exact.*

To get a better grip on exactness, it is also worth verifying that the first isomorphism theorem of groups (written multiplicatively) is equivalent to the fact that if $\pi(H) \trianglelefteq G$, then:

$$1 \to H \xrightarrow{\pi} G \xrightarrow{\tau} G/H \to 1$$

is short exact.

Suppose that M_1 and M_2 are two R-modules. We define the **direct sum** $M_1 \oplus M_2$ to be the R-module with coordinatewise addition and multiplication. We get two submodules $\{0_{M_1}\} \oplus M_2$ and $M_1 \oplus \{0_{M_2}\}$ for free, and in fact we get a short exact sequence for free! Indeed, the sequence:

$$0 \to M_1 \xrightarrow{i} M_1 \oplus M_2 \xrightarrow{p} M_2 \to 0$$

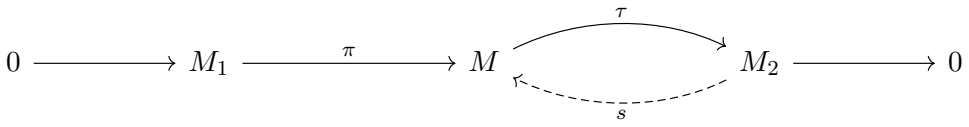
is short exact, and in this case we say that the short exact sequence **splits**. Splitness is a good way of verifying whether or not a module can be decomposed, but this does not work for even straightforward modules (although it always works for vector spaces!). If we let $R = \mathbb{Z}$ and $n \in \mathbb{N}$, the short exact sequence:

$$0 \to \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \xrightarrow{p} \mathbb{Z}/n\mathbb{Z} \to 0$$

is *not* split; it is not possible that $\mathbb{Z} \cong \mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, as there is no copy of $\mathbb{Z}/n\mathbb{Z}$ inside $\mathbb{Z}$, but $\mathbb{Z}/n\mathbb{Z} \cong \{0_{\mathbb{Z}}\} \oplus \mathbb{Z}/n\mathbb{Z} \subseteq \mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. So when does a short exact sequence split?

To move forward, we define a **section** of a morphism f in a category C to be any right inverse of f. *Caution!* This right inverse must be a morphism of C, not just Set.

Theorem 29. *A short exact sequence S of R-modules:*



splits if and only if there is a section s of τ in R-Mod.

Proof. We first suppose that S splits; i.e., that $M \cong M_1 \oplus M_2$. Write M in such a fashion, so each $m \in M$ is some $(m_1, m_2) \in M_1 \oplus M_2$.

We wish to find a section, and to that end, let $s(y) = (0, y)$. Clearly s is an R-module homomorphism, and since $\tau(x, y) = y$ for all $(x, y) \in M_1 \oplus M_2$, it follows that $\tau(s(y)) = y$ for every $y \in M_2$, so s is a section in Set, hence by homomorphism a section in R-Mod.

$$(x, y) \xmapsto{d} \pi(x) + s(y)$$

We claim d certifies $M_1 \oplus M_2 \cong M$. That d is a homomorphism follows from commutativity of $+$, distributivity of $\cdot$, and that π and s are homomorphisms.

To show injectivity, we see that $\ker(d) = \{(x, y) : \pi(x) = -s(y)\}$, so it amounts to showing that any (x, y) so that $\pi(x) = -s(y)$ is $(0, 0)$. Indeed, this condition implies

that $\tau(\pi(x)) = -\tau(s(y)) = -y$, so by exactness (that $\text{im}(\pi) = \ker(\tau)$) it follows that $y = 0_{M_2}$, so since s is a homomorphism, $\pi(x) = 0_M$, and again by exactness π is injective, so $x = 0_{M_1}$. Thus $\ker(d) = \{(0, 0)\}$, so d is injective.

To see surjectivity, suppose $z \in M$. We want $x \in M_1$ and $y \in M_2$ so that $z = \pi(x) + s(y)$. In other words, we want x and y so that $\pi(x) = z - s(y)$, so it suffices to find y that $z - s(y) \in \text{im}(\pi)$. This is not bad: let $y = \tau(z)$. Then $\tau(z - s(y)) = \tau(z) - \tau(s(y)) = 0$, so $z - s(y) \in \ker(\tau) = \text{im}(\pi)$.

Thus d is a bijection, proving that S splits.

□

Notice that nowhere we explicitly used that τ is surjective– we could have, but instead let it live implicitly in the fact that s is a section.

As alluded to by the proof, this justifies that every short exact sequence of vector spaces splits; if W is a vector subspace of V, the following sequence:

$$0 \to W \to V \to W^{\perp} \to 0$$

splits, and in fact, a choice of s sends elements of $V/W \cong W^{\perp}$ to $W^{\perp}$ itself living in V.

4.3 3/7/22: Particularly Nice Kinds of Modules

Suppose that M is an R-module. We say that an R**-linear combination** of $\{m_1, \ldots, m_n\} \subseteq M$ is any sum of the form $\sum_{i=1}^{n} r_i m_i$, where $r_i \in R$ for all i.

The first Particular Nice Kind of Module we've encountered is a module over a field K; i.e., a vector space. Every vector space has a basis, and it is a tragedy that this does not hold even for relatively well-behaved modules. We will be discussing the next best thing– considering an n-basis as equivalent to a bijection $K^n \to V$, we will consider the case when there is only a surjection $R^n \to M$.

In other words, we call an R-module M **finitely generated** if there exists a **generating set** $\{m_i\}_{i=1}^{k}$ so that every $m \in M$ is an R-linear combination of the m_i; i.e, that $\langle m_1, \ldots, m_k \rangle = M$.

We can refine this notion by saying that an R-module is n**-generated** if there are $m_1, \ldots, m_n$ so that $\langle m_1, \ldots, m_n \rangle = M$.

The following theorem illustrates the theory of n-generated modules— it's quite pretty, and we add some extra exposition to illustrate the interplay between concepts and rigor.

Theorem 30. *There is a 1-1 correspondence between 1-generated R-modules and quotient rings R/I, formed by isomorphisms.*

Proof. Suppose M is 1-generated. Then there is some m so that $M = \langle m \rangle$. Clearly if m should correspond to some ideal, then it should be "invariant under translation" by R. Hence consider the translation R-module homomorphism $f : R \to M$ with the rule:

$$f(r) = rm$$

Paying attention to what lives where, we see that $\ker(f)$ is a submodule of R over R (!), and as $M = \langle m \rangle$, f is surjective, so by the Fundamental Homomorphism Theorem for Modules:

$$M = f(R) \cong R/I$$

but R/I as R-modules is just R/I as a ring!

For the other direction, suppose that $M \cong R/I$ for some submodule (ideal) I. Then there is an isomorphism $i : R/I \to M$.

Since every $r \in R$ (as a ring) can be written $r \cdot 1_R$ (as a module), for every $[r] \in R/I$ (as a ring) we see that $[r] = r \cdot [1]_M$ (as a module), thus as a module, $R/I = \langle [1] \rangle$, so $M = \langle i([1]) \rangle$. □

This gorgeous theorem basically kills any potential for a theory of 1-generated modules, relegating it to a theory of rings. Studying n-generated modules for fixed n seems painful, so we will move on to finite generation. However, even this is not that nice– a finitely generated module does not necessarily have finitely generated submodules, which stymies useful decompositions. Hence we pass to the next best Particularly Nice Kind of Module: Noetherian modules.

If M is an R-module, we say that M is **Noetherian** if every R-submodule of M is finitely generated.

As with many module definitions, this specializes pleasantly to **Noetherian** rings, which are Noetherian R-modules R. Translated, this is equivalent to saying that every ideal of R is finitely generated. As it turns out, there are a few useful ways of thinking about Noetherianness.

Theorem 31. *Suppose that M is an R-module. Then the following are equivalent:*

1. *M is Noetherian.*
2. *Every increasing chain of R-submodules of M stabilizes.*
3. *Every nonempty subposet of $(\{N : N \leq M\}, \subseteq)$ has a maximal element.*

Proof. First we show (1) implies (2). Take any increasing chain $C = \{M_n\}_{n\in\mathbb{N}}$ of R-submodules of M; by Lemma 16, $M_\infty := \bigcup C$ is an R-submodule of M. By (1), $M_\infty = \langle m_1, \ldots, m_k\rangle$ for some $m_i \in M$, so at most $k-1$ containments in C are strict; i.e., the sequence stabilizes.

To see (2) implies (3), we show the contrapositive. Let $\varnothing \neq S \subseteq (\{N : N \leq M\}, \subseteq)$ have no maximal element. Pick any $M_1 \in S$. Since S has no maximal element, there is some $M_2 \in S$ so that $M_1 \subsetneq M_2$. Carrying on in this fashion, we obtain a sequence of nested submodules:

$$M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \ldots \qquad (*)$$

which never stabilizes.

Now we show (3) implies (1), completing the proof. Suppose that N is a submodule of M. Consider $\mathcal{F}$, the set of finitely-generated submodules of N. Since $\{0\} \in \mathcal{F}$, we may apply (3) to obtain a maximal element $\top \in \mathcal{F}$.

If there were some $q \in N$ which were not in $\top$, then $\top \subsetneq \langle \top, q\rangle$, contradicting maximality. Hence $\top = N$, so N is finitely generated, so every submodule of M is finitely generated. □

A bit of culture can be explored by way of step $(*)$. Certainly one can justify finding a finite-length sequence by induction, but a transfinite sequence requires something more. The mathematician immediately jumps to Choice, but it turns out a much weaker variant is all that is necessary.

A binary relation on X^2 is called **entire** if for every $a \in X$, there is some $b \in X$ so that aRb is true.

Axiom of Dependent Choice. *For every nonempty set X and entire binary relation R on X^2, there exists a sequence $(x_n)_{n\in\mathbb{N}}$ in X so that:*

$$xRx_{n+1}, \forall n \in \mathbb{N}$$

Observe this implies choice for countable index sets, and is necessary to construct such a "chain" as in step $(*)$. One can do most of real analysis with Dependent Choice, but among the (infinite) set of things which require Choice, Dependent Choice is not strong enough to construct a non-Lebesgue-measurable set. Real measure theory must be quite pleasant in $\mathsf{ZF}(\mathsf{DC})$!

Back to module theory.

We get for free from Theorem 31:

Corollary 9. *The conditions of Theorem 31 (mutatis mutandis) characterize Noetherian rings.*

Continuing our search for Particular Nice Kinds of Modules, we consider the question of how generation of the coefficient ring R constrains generation of M. The following is a partial answer.

Theorem 32. *Suppose R is a Noetherian ring. Then an R-module M is Noetherian if and only if M is finitely R-generated.*

Proof. The forward direction holds for any R, not just Noetherian R. The hard part will be the other direction, and it proceeds in an interesting fashion.

Suppose that $M = \langle x_1, \ldots, x_n \rangle$. Then the sequence:

$$R^n \xrightarrow{f} M \to 0$$

is short exact, where $f(r_1, \ldots, r_n) = \sum_{i=1}^{n} r_i x_i$. We claim it suffices to show that R^n over R is a Noetherian module. We proceed by induction on n. The basic intution is that we should be able to break up R^n into $R^{n-1} \text{“}\oplus\text{”} R$, apply induction, and combine the generators to obtain a finite generating set for submodules of R^n. The actual answer ends up being a little more complicated.

Suppose that $P \leq R^n$ is a submodule. Consider the projection $p : R^n \to R^{n-1}$:

$$p(x_1, \ldots, x_n) = (x_1, \ldots, x_{n-1})$$

This is an R-module homomorphism, hence $p(P) \leq R^n$. By induction, $p(P) = \langle q_1, \ldots, q_k \rangle$, where $q_i \in p(P) \subseteq R^{n-1}$.

Since p is surjective, we can find $b_i \in P$ so that $p(b_i) = q_i$. Thus for every $c \in P$, we can find $r_1, \ldots, r_k$ so that:

$$f(x) = \sum_{i=1}^{k} r_i f(b_i)$$

In other words:

$$f\left(x - \left(\sum_{i=1}^{k} r_i b_i\right)\right) = 0$$

so $x - \left(\sum_{i=1}^{k} r_i b_i\right) \in \ker(f)$, and certainly is in $\ker(f) \cap P$. Since the intersection of submodules is a submodule, it follows that $\ker(f) \cap P \leq R$, so by induction $\ker(f) \cap P = \langle d_1, \ldots, d_l \rangle$.

Hence $x - \left(\sum_{i=1}^{k} r_i b_i\right) = \sum_{j=1}^{l} r'_j d_j$, so $x \in \langle b_1, \ldots, b_n, c_1, \ldots, c_l \rangle$, thus P is finitely generated.

The f of the above exact sequence will carry R^n's Noetherianness into M; indeed, since f is surjective, it follows that for every $N \leq M$, $N = f(f^{-1}(N))$. But $f^{-1}(N)$ is a submodule of R^n over R, hence $f^{-1}(N) = \langle z_1, \ldots, z_c \rangle$, and as f is a surjective homomorphism, it follows that, as promised:

$$N = \langle f(z_1), \ldots, f(z_c) \rangle$$

□

This is a pretty complete answer for Noetherian rings over finitely generated modules—Noetherian modules are extremely well-behaved, and their Noetherianness is generally preserved under module operations. This in mind, it makes sense to specialize to an Extra Nice Kind of Module: a module over a PID.

We say that an R-module M is **finitely presented** if there an exact sequence:

$$R^k \xrightarrow{\tau} R^n \xrightarrow{f} M \to 0$$

That $R^n \xrightarrow{f} M \to 0$ is exact tells us that M is finitely generated, and $R^k \xrightarrow{\tau} R^n \xrightarrow{f} M$'s exactness tells us something more: that $\ker(f)$ is finitely generated! To understand the significance of this, we need to return to basics.

The cyclic group of order n can be written as $\{a : a^n = 1\}$. This is a pretty nice way of writing $\mathbb{Z}/n\mathbb{Z}$, as it makes no reference to ambient group structures, and encodes all information. This notion is what we seek. We say that a **presentation** of a group G comprises a set S of generators, and R of relations among S. We write $G = \langle S | R \rangle$, so in the case above, we can write $\langle a | a^n = 1 \rangle$, or more briefly, $\langle a | a^n \rangle$. Another example shows the power of this abstraction: the complexity of D_n, the group of symmetries of a regular n-gon, can be written:

$$\langle r, f | r^n, f^2, (rf)^2 \rangle$$

But how does one arrive at a presentation? We can always define the **free group on 2 symbols** F_2, presented $\langle s_1, s_2 \rangle$, and then we can quotient by the normalizer N of the strings which we would become 1 in D_n. If R generates this subgroup, it follows that:

$$F_2/N = \langle s_1, s_2 | R \rangle \cong D_n$$

Now we push the motivation up to the level of modules. In this case, R is finite if and only if $\ker(f)$ is finitely generated, so finite presentation of modules is precisely

what we would expect now: M is finitely presented if and only if it is the quotient of a free module by finitely many "relations;" i.e., elements of $\ker(f)$.

It turns out that restricting the generation of the coefficient ring has great bearing on the presentation of a module– this can be seen by the double appearance of R in the exact sequence which certifies finite presentation.

For example, if a module M over a Noetherian ring is finitely generated, it follows that it is finitely presented. After all, $\ker(f)$ is finitely generated as an R-submodule of R^n over R, so we can find a k so that R^k's generators are sent to the generators of $\ker(f)$. This construction is given explicitly in the next paragraph.

We will proceed in a general construction of encoding the presenting relations of a module over a PID, but first, we give a motivating example: that of a finitely generated $\mathbb{Z}$-module M; i.e., an abelian group. Since M is essentially a finitely generated abelian group, finite presentation follows for free. After all, if $M = \langle m_1, \ldots, m_n \rangle$, then the coefficient surjection f onto the generators gives a short exact sequence:

$$\mathbb{Z}^n \xrightarrow{f} M \to 0$$

which may be extended to a certification of finite generation:

$$\mathbb{Z}^k \xrightarrow{\tau} \mathbb{Z}^n \xrightarrow{f} M \to 0$$

Where if we write $\ker(f) = \langle a_i, \ldots, a_k \rangle$, the map τ is defined $\tau(\mathbf{e}_i) = a_i$. It follows that we can determine the entire structure of M (this is why we like finite presentation!) by the matrix:

$$A = \begin{bmatrix} | & & | \\ \mathbf{a}_1 & \cdots & \mathbf{a}_k \\ | & & | \end{bmatrix}$$

by short exactness. After all, if given such an A, we can form $I = \langle \mathbf{a}_1, \ldots, \mathbf{a}_k \rangle \subseteq \mathbb{Z}^n$, and obtain from the sequence that $M \cong \mathbb{Z}^n / I$, a complete description of M.

In general, such an A is not unique, and like the Jordan normal form, we are interested in finding a standard representative which has useful properties.

To finish this section, we state the goal. For a module M over a PID R, we claim there is a standard diagonal representative:

$$A = \begin{bmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{bmatrix}$$

called the **Smith normal form of** A whose columns generate $\ker(f)$ in the finite presentation exact sequence, and so that $a_1 | a_2 | \cdots | a_n$. Moreover, A is unique up to reordering diagonal entries.

Hence modules over PID's are the latest Particularly Nice Kind of Module, and as is clear from this exposition, are at least an Extremely Nice Kind of Module.

4.4 3/9/22: The Smith Normal Form: Understanding Modules over PID's

We quickly summarize the discussion of Section 4.3. We say that an R-module M is **finitely presented** if there are n and k so that the sequence:

$$0 \to R^k \xrightarrow{\tau} R^n \xrightarrow{f} M \to 0$$

is short exact. However, since short exactness entails that τ is injective, we can think of R^k above as just $I = \ker(f)$. That is to say, we can rewrite the above in the form:

$$0 \to I \xrightarrow{\text{"id"}} R^n \xrightarrow{f} M \to 0$$

Since the sequence is short exact, if R is Noetherian it follows that I is finitely generated, so if $I = \langle \mathbf{a}_1, \ldots, \mathbf{a}_n \rangle$, it follows that we can express these generators as:

$$A = \begin{bmatrix} | & & | \\ \mathbf{a}_1 & \cdots & \mathbf{a}_k \\ | & & | \end{bmatrix}$$

and if R is the best kind of Noetherian ring—a PID—we can say A is generator-equivalent to a Smith normal form with diagonal entries $c_1, \ldots, c_k$, hence $M \cong R^n / \langle \mathbf{c}_1, \ldots, \mathbf{c}_k \rangle$ for easy vectors $(\mathbf{c}_i)_j = c_i$ if $j = i$ and 0 else.

We now provide an explicit computation, which may elucidate the construction.

Let G be a finitely generated abelian group (finitely generated $\mathbb{Z}$-module), hence finitely presented with say, presentation:

$$G = \langle g_1, g_2, g_3 | (5g_1 + 2g_2 + 3g_3), (3g_2 + 2g_3) \rangle$$

By the above discussion, this is nothing but the claim that:

$$G \cong \mathbb{Z}^3 / \langle \mathbf{a}_1, \mathbf{a}_2 \rangle$$

where $\mathbf{a}_1 = \begin{bmatrix} 5 \\ 2 \\ 3 \end{bmatrix}$ and $\mathbf{a}_2 = \begin{bmatrix} 0 \\ 3 \\ 2 \end{bmatrix}$. The goal is to find better generators. In fact, by changing the generators to Smith normal generators, *we find a representation of G as a direct sum of cyclic groups.* This is significant, and bodes well for a high-powered corollary of the general construction for modules.

Thus we want:

$$\begin{bmatrix} 5 & 0 \\ 2 & 3 \\ 3 & 2 \end{bmatrix} \xmapsto{\text{generator-preserving operations}} \begin{bmatrix} c_1 & 0 \\ 0 & c_2 \\ 0 & 0 \end{bmatrix} \text{ s.t. } c_1 | c_2$$

To inspect: [Here Borisov says that elementary row operations preserve generators, as a sufficient condition is that R is a Euclidean domain. This doesn't seem right–perhaps PID is what is needed.]

The computation is as follows:

$$\begin{bmatrix}5 & 0\\ 2 & 3\\ 3 & 2\end{bmatrix} \overset{R_2\leftrightarrow R_1}{\longmapsto} \begin{bmatrix}2 & 3\\ 5 & 0\\ 3 & 2\end{bmatrix} \overset{-(R_1-R_3)}{\longmapsto} \begin{bmatrix}1 & -1\\ 5 & 0\\ 3 & 2\end{bmatrix} \overset{C_2+C_1}{\longmapsto} \begin{bmatrix}1 & 0\\ 5 & 5\\ 3 & 5\end{bmatrix} \overset{R_2-5R_1,R_3-3R_1}{\longmapsto} \begin{bmatrix}1 & 0\\ 0 & 5\\ 0 & 5\end{bmatrix} \mapsto \begin{bmatrix}1 & 0\\ 0 & 5\\ 0 & 0\end{bmatrix}$$

Thus we obtain a much, much nicer presentation of G:

$$G = \langle h_1, h_2, h_3 | h_1, 5h_2 \rangle$$

Hence $G \cong \mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$. The proof of the Smith normal form is not that terrible, but involves some algorithmic computation– the hardest part is conceptually understanding the correspondence of columns of the normal form with the relations in M's presentation. Thus we are more than ready to prove:

Theorem 33 (Smith Normal Form)**.** *Suppose that R is a PID, and $A \in M_n(R)$. Then there are invertible J_1, J_2 (compositions of row and column operations, respectively) so that:*

$$J_1 A J_2 = \begin{bmatrix} c_1 & & & & & & \\ & c_2 & & & & & \\ & & \ddots & & & & \\ & & & c_k & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}$$

where $c_1 | c_2 | \cdots | c_k$. Moreover, the c_i are unique up to units in R, and the normal form is unique up to rearrangement.

We will prove this with the help of the following lemma:

Lemma 19. *Let $A, B \in M_n(R)$. Then an $n \times n$ minor of AB is a linear combination of the $n \times n$ minors of B.*

Proof. Recall that rows of AB are linear combinations of rows of B. After all, A encodes a number of row operations on B.

The key observation is that that linear combination descends to the submatrix Q of AB which induces an $m \times m$ minor of AB, as a minor must uniformly omit or include columns.

If we write the linear combinations as $r_j(Q) = \sum_{l=1}^{n_j} \alpha_{l,j} r_{i_{l,j}}(B)$, then it follows from row-multilinearity of the determinant that:

$$\det(Q) = \det \begin{bmatrix} \sum_{l=1}^{n_1} \alpha_{l,1} r_{i_{l,1}}(B) \\ \vdots \\ \sum_{l=1}^{n_m} \alpha_{l,m} r_{i_{l,m}}(B) \end{bmatrix} = \sum_{q=1}^{m} \sum_{l=1}^{n_q} \alpha_{l,q} \det \begin{bmatrix} r_{i_{l,q}}(B) \\ \vdots \\ r_{i_{l,q}}(B) \end{bmatrix}$$

Since the right-hand determinants are $n \times n$ minors of B, and a linear combination of linear combinations is a linear combination, the result follows. □

Moreover, we will be repeatedly and implicitly using:

Lemma 20. *The following row and column operations preserve the finitely generated module I over a PID (up to isomorphism):*

1. *Switching rows and columns.*
2. *Adding λ of one column to another.*
3. *Adding μ of one row to another.*

Parts (1) and (2) are easy, but (3) seems less naively obvious. I'm pretty sure that there's something to be said about left-multiplication by an element of $GL_n(R)$ being an R-module isomorphism, but I can't be bothered— this would require a few intermediary lemmas relating matrices with entries in R to R-module homomorphisms, and I'm willing to take Lemma 20 on faith that this theory works.

Now we will verify Theorem 33.

Proof. The proof of existence is algorithmic in nature, hence proved by induction on the size of A.

Suppose that $A \neq \mathbf{0}$. Up to a rearrangement of the order of generators, and a permutation of coordinates, we may assume that $a_{11} \neq 0$; i.e., writing A in the form:

$$\begin{bmatrix} a_{11} & \mathbf{b} \\ \mathbf{c} & D \end{bmatrix}$$

For the purpose of this proof, we will say that an entry a of A, is **refined with respect to** B, where B is a submatrix of A, if $a|b$ for all entries b in B. Then we may present the algorithm to obtain Smith normal form:

1. Permute A to obtain $a_{11} \neq 0$, and partition A as above.
2. Apply row and column operations to clear $\mathbf{b}$ and $\mathbf{c}$.
3. Refine a_{11} with respect to D.
4. Repeat for the respective submatrix D until A is in Smith normal form.

Now we must justify that we can perform steps 2-4 (as we have already justified 1), and then apply induction to D to finish the proof. We will first show that we may refine a_{11} with respect to $\mathbf{c}$, and in the process annihilate $\mathbf{c}$, and conclude by symmetry we may do the same with respect to $\mathbf{b}$.

Indeed, suppose there exists some $j > 1$ so that a_{11} does not divide a_{j1}. We claim we can find q so that $q|a_{11}$ and $q|a_{j1}$, and then find a row operation to send a_{11} to q and a_{j1} to 0.

The assumption that R is a PID here is essential, as we may always find $q = \gcd(a_{11}, a_{j1})$, and by Bezout's Lemma for PID's, we can find u and v in R so that $a_{11}u + a_{j1}v = q$.

Let $\alpha_1 = a_{11}/q$ and $\alpha_j = a_{j1}/q$; by Bezout's Lemma, it follows that:

$$\alpha_1 v + \alpha_j u = 1 \tag{4.1}$$

This is enough to guarantee the invertible transformation we seek; if we select Q carefully, it follows that:

$$Q \begin{bmatrix} a_{11} \\ a_{j1} \end{bmatrix} := \begin{bmatrix} u & v \\ -\alpha_j & \alpha_1 \end{bmatrix} \begin{bmatrix} a_{11} \\ a_{j1} \end{bmatrix} = \begin{bmatrix} a_{11}u + a_{j1}v \\ \alpha_1 a_{j1} - \alpha_j a_{11} \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}$$

and since $\det(Q)$ is just Equation 4.1, it follows that Q is invertible.

In other words, Q encodes the row operations involving Row 1 and Row j which results in reducing a_{11} to $\gcd(a_{11}, a_{j1})$ and clears a_{j1}. Proceed in this fashion for each j (and similarly right-multiply for each i) to reduce A to:

$$\begin{bmatrix} c_{11} & \mathbf{0} \\ \mathbf{0} & D' \end{bmatrix}$$

If all elements of D' are divisible by c_{11}, we are done, as above algorithm preserves that divisibility. If there exists an entry of D' which c_{11} does not divide, we can add its row to Row 1, then apply the above process. Hence c_{11} divides D', and by induction on D we are done with existence.

Uniqueness (as usual) has a different flavor.

Let $D_i(A)$ be the set of $i \times i$ minors of A, and define $d_i(A) = \gcd(D_i(A))$. Uniqueness will follow from the claim that $d_i(A) | d_i(JA)$ for every $J \in M_n(R)$. Indeed, by Lemma 19, every $i \times i$ minor of JA is a linear combination of minors of A, hence every minor of JA is a multiple of $D_i(A)$, thus by definition of the gcd it follows that $D_i(JA)$ is a multiple of $D_i(A)$.

Now suppose that J is invertible; then $D_i(JA)$ divides $D_i(J^{-1}JA) = D_i(A)$, so if J is invertible, our conclusion that $D_i(A) | D_i(JA)$ implies that $D_i(A) = D_i(JA)$.

Moreover, using an analogue of Lemma 19 on A's columns we can obtain (by symmetric means) that $D_i(A) = D_i(AJ)$.

In particular, if S is A's Smith normal form:

$$S = \begin{bmatrix} c_1 & & & & & & \\ & c_2 & & & & & \\ & & \ddots & & & & \\ & & & c_k & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix},$$

it follows that $D_i(S) = D_i(A)$ for each $i \in [n]$. What is the purpose of these gcd's? Observe that, by construction, $c_1 = D_1(S)$.

In fact, we can say something better: for each $i \in \{2, \dots, n\}$, $c_i = D_i(S)/D_{i-1}(S)$. This because $c_1|c_2|\dots|c_k$, therefore:

$$D_i(S) = \gcd\left(\prod_{\substack{I \in \binom{[k]}{i} \\ q \in I}} c_q\right) = \prod_{q=1}^{i} c_q$$

Thus $D_i(S)/D_{i-1}(S) = \prod_{q=1}^{i} c_q / \prod_{q=1}^{i-1} c_q = c_i$.

This gives what we wish for uniqueness: c_i is $D_i(A)/D_{i-1}(A)$, which is determined by $\{D_i(A)\}_{i\in[n]}$, modulo units.

□

4.5 3/11/22: The Structure Theorem for Finitely Generated Modules over PID

The Smith normal form is a good example of why f.g. modules over PID's are special, but the following "corollary" is even better:

Theorem 34 (Classification of f.g. Modules over a PID)**.** *Suppose that R is a PID and M is a finitely generated R-module. Then:*

$$M \cong \bigoplus_{i=1}^{N} R/\langle a_i \rangle$$

where $a_1|a_2|\dots|a_N$, and a_1 is a nonunit. Moreover, the a_i are unique up to units.

The existence follows from the Smith normal form; uniqueness is harder to prove. Here is how we shall do it:

1. We will prove there exists an alternative decomposition into primary cyclic modules (to be defined!) induced by the Chinese Remainder Theorem.
2. We will break up the direct sum of Theorem 34 into a sum of cyclic-like summands, and non-cyclic-like summands.
3. We will show existence of this decomposition by the Smith normal form.
4. We will show the cyclic-like part is unique:
   (a) We will form an algorithm which uniquely forms an isomorphism between a decomposition into a direct sum of primary cyclic modules, and a Smith decomposition.
   (b) We will use a Jordan-like approach to show that the primary cyclic representation of the cyclic-like part is unique.
   (c) It follows that the cyclic-like part itself is unique, hence so is its Smith decomposition.
5. We will show the non-cyclic-like part is unique, using tools from linear algebra.

We have seen the Chinese Remainder Theorem for rings before, and as a ring is a module, it should follow that there is a Chinese Remainder Theorem for modules as well. In fact, since submodules are better-behaved in certain respects than ideals, the following theorem for modules over PID's is sleek:

Theorem 35 (Chinese Remainder Theorem for Modules)**.** *Suppose that $b_1, \dots, b_k$ are pairwise coprime in R. Then:*

$$R/\langle b_1 \dots b_k \rangle \cong \bigoplus_{i=1}^{k} R/\langle b_i \rangle$$

Proof. The case $k = 2$ follows the proof of the CRT for rings, with appropriate adjustments of language. For $k > 2$, by the $k = 2$ case and induction:

$$R/\langle b_1 \dots b_k \rangle \cong R/\langle b_1 \rangle \oplus R/\langle b_2 \dots b_K \rangle \cong \bigoplus_{i=1}^{k} R/\langle b_i \rangle$$

□

The finest decomposition of a module through Theorem 35 has as its b_i the "minimally coprime factors of $b_1 \dots b_k$;" i.e., the prime factors of highest power. Hence such a module deserves a name: if a module M over a PID R is of the form $R/\langle p^k \rangle$ for some p prime, we say that M is a **primary cyclic module**.

Hence we can restate Theorem 35:

Corollary 10 (Theorem 35, Restated)**.** *Suppose R is a PID and $q \in R$. If $\{p_i^{\alpha_i}\}_{i\in[n]}$ is q's prime factorization, then R has the decomposition into primary cyclic modules:*

$$R/\langle q \rangle \cong \bigoplus_{i=1}^{n} R/\langle p_i^{\alpha_i} \rangle$$

This is evidently unique. We will next define a **free R-module** as an R-module which has a basis set S which is linearly independent, and R-spans M.

The generality of the above definition is largely for flavor; the free module we will work with is R over R, for which any unit is a basis.

Define the **torsion submodule** of a module M to be:

$$\mathrm{Tor}(M) = \{x \in M : \exists a \neq 0 \in R \text{ s.t. } ax = 0\}$$

It's not hard to show that $\mathrm{Tor}(M)$ is closed under addition and scaling, so we will omit the proof that it is indeed a submodule.

Lemma 21 (Step 3 of the Proof of Theorem 34)**.** *Suppose R is a PID and M is finitely generated, then:*

$$M \cong \mathrm{Tor}(M) \oplus R^r$$

Proof. This follows from the Smith normal form theory; simply write $M \cong \bigoplus_{i=1}^{N} R/\langle a_i \rangle$ where $a_1 | a_2 | \dots | a_N$, and observe that if k is the largest index where $a_k \neq 0$, then:

$$\bigoplus_{i=1}^{N} R/\langle a_i \rangle = \bigoplus_{i=1}^{k} R/\langle a_i \rangle \oplus R^{N-k}$$

To finish the proof, we must only show that $\mathrm{Tor}(M) = \bigoplus_{i=1}^{k} R/\langle a_i \rangle$. Indeed, if $x \in \bigoplus_{i=1}^{k} R/\langle a_i \rangle$, then $a_k x = 0$ (observe this requires the nice divisibility relation given by the Smith normal form), so $x \in \mathrm{Tor}(M)$. On the other hand, if $x \in \mathrm{Tor}(M)$, certainly $x \notin R^r$, so $x \in \bigoplus_{i=1}^{k} R/\langle a_i \rangle$. □

Lemma 22 (Step 4a of the Proof of Theorem 34)**.** *There is a unique 1-1 correspondence, given by the Chinese Remainder Theorem, between a Smith decomposition:*

$$\bigoplus_{i=1}^{k} R/\langle a_i \rangle \text{ s.t. unit} \neq a_1|a_2|\ldots|a_k \neq 0$$

and a decomposition into primary cyclic modules:

$$\bigoplus_{j=1}^{l} R/\left\langle p_j^{k_j} \right\rangle$$

up to a permutation of coordinates and scaling by units.

This is algorithmic, and we omit a proof. [**Watch the lecture for an example, and practice!!**]

Lemma 23 (Step 4b of the Proof of Theorem 34)**.** *There is a representation of* $\mathrm{Tor}(M)$ *as a direct sum of primary cyclic modules, and it is unique.*

Proof. As we have seen in Lemma 21, we may write $\mathrm{Tor}(M)$ in a nondegenerate Smith decomposition (i.e, no quotients by zero ideals). By Lemma 22, we may associate this decomposition uniquely with a decomposition into primary cyclic modules (PCD). Now we will use a method familiar from Jordan normal form theory to show that that M's PCD is unique (up to units, of course).

We get for free from Theorem 35 that the relevant primes are unique in their occurrence. Thus it remains to guarantee that the number of times a given quotient by a power of that prime appears in the sum is uniquely determined by M.

Observe that $F = R/\langle p_i \rangle$ is a field, as $\langle p_i \rangle$ is a prime, hence maximal, ideal in the PID R.

Next, let t_p be a translation map which left-multiplies by p. Letting $M_{p^j} = p^j M \cap \ker(t_p)$, it follows that M_{p^j} is a vector space over F. Next, observe two facts: if $M = R/\langle q^n \rangle$ where p does not divide q^n, then $\ker(t_p : M \to M) = \{0\}$. On the other hand, If $M = R/\langle p^m \rangle$, then $\ker(t_p : M \to M) = \left\langle [p^{m-1}] \right\rangle$. Hence:

$$p^j(R/\left\langle p^i \right\rangle) \cap \ker(t_p : R/\left\langle p^i \right\rangle \to R/\left\langle p^i \right\rangle) \cong \begin{cases} \{0\} & \text{if } j \geqslant i \\ R/\langle p \rangle & \text{if } j < i \end{cases}$$

Thus if we know that $M \cong \bigoplus_{i=1}^{n} R/\left\langle p_i^{k_i} \right\rangle$, then we apply the above relation to M to count the number of times that $p_i^{k_i}$ appears. However, due to divisibility concerns, if a higher power of p also appears a number of times, we will have counted the occurrences of all higher powers, so we simply take differences of the count for each power.

This results in a unique number, hence the decomposition is unique.

□

Corollary 11 (Step 4c of the Proof of Theorem 34)**.** *The representation of* $\mathrm{Tor}(M)$ *given by the Smith decomposition is unique.*

Proof. We use Lemma 23 to get a unique primary cyclic decomposition, then pull back via Lemma 22 to obtain a unique Smith decomposition. However, this was the one we started with, so it is unique after all. □

Lemma 24 (Step 5 of the Proof of Theorem 34)**.** *The r of the decomposition in Lemma 21 is uniquely determined by M.*

Proof. We know that $\mathrm{Tor}(M)$ is uniquely determined by M, hence by the decomposition, $R^r = M/\mathrm{Tor}(M)$ is uniquely determined by M. Thus this amounts to the claim that if R is commutative (which we will use implicitly), then $R^{r_1} \cong R^{r_2}$ implies $r_1 = r_2$. To see this, we will work through the vector space $Q(R)$ over $Q(R)$.

Indeed, if $r_1 < r_2$, and suppose for contradiction that $R^{r_1} \cong R^{r_2}$. Then there are $x_1, \ldots, x_{r_2} \in R^{r_1} \subsetneq Q(R)^{r_1}$ so that for all $n_1, \ldots, n_{r_2}$ nonzero,

$$n_1 x_1 + \cdots + n_{r_2} x_{r_2} \neq 0$$

After all, just take an image of a basis under the module isomorphism $R^{r_2} \to R^{r_1}$.

But as $\dim(Q(R)^{r_1}) = r_1$, this is impossible: such a set of vectors must span $Q(R)^{r_1}$, hence contain 0 in their span. Thus $R^{r_1} \ncong R^{r_2}$.

Apply the symmetrical reasoning and take contrapositives to finish the proof. □

Now we prove Theorem 34.

Proof. By Lemma 21, M may be represented by the Smith decomposition of its kernel relations. By Corollary 11, the torsion part of the direct sum is unique, and by Lemma 24, the free part is unique. □

Hence we have proved the Classification Theorem for Finitely Generated Modules over Principle Ideal Domains, sometimes referred to as "The Structure Theorem."

One (huge!) corollary is to consider the isomorphism between finitely generated abelian groups and finitely generated $\mathbb{Z}$-modules, hence obtaining:

Corollary 12 (Classification of Finitely Generated Abelian Groups)**.** *Every finitely generated abelian group can be expressed uniquely as a direct sum of cyclic groups, either given by the Chinese Remainder Theorem, or the Smith decomposition.*

4.6 3/21/22: Some Corollaries of the Structure Theorem

This lecture was kind of messy to me, but hopefully everything here makes sense.

Today, we will be proving the existence and uniqueness for the Jordan normal form as a corollary of the Structure Theorem. In fact, this might give some more insight into "why" we did what we did in the proof.

Consider any linear operator $L : V \to V$; i.e., any endomorphism of the $\mathbb{C}$-module V.

Theorem 36. *There is a one-to-one correspondence between pairs (V, L) and $\mathbb{C}[t]$-modules given by $(V, L) \mapsto (V, +, *)$, where for every $f \in \mathbb{C}[t]$ and $\mathbf{v} \in V$, $f * \mathbf{v} = f(L)\mathbf{v}$.*

For flavor, this correspondence will work between $(V, \{L_i\}_{i\in[n]})$ and $\mathbb{C}[t_1, \ldots, t_n]$-modules if and only if the L_i pairwise commute.

Proof. First, we can sanity-check that $(V, +, *)$ is a module– this follows from linearity (alternatively, endomorphic properties) of L. In fact, this gives the forward direction!

To see the backwards direction, suppose M is a $\mathbb{C}[t]$-module. Then M is also a $\mathbb{C}$-module, and we can define $L : M \to M$ by $L(x) = tx$. By the module axioms, L is an endomorphism. □

For more flavor, this is technically an equivalence of categories between $\mathbb{C}[t]$-Mod and $\mathsf{Vec}(V, L)$, where the second category has as its morphisms those which commute with L.

This result holds for every vector space! On the other hand, if we wish to leverage the tools of module theory to understand vector spaces, this is not very helpful. Indeed, we need to place weighty restrictions on the nature of the module in the correspondence to obtain a nicer vector space.

Theorem 37. *The bijection of Theorem 36 induces a one-to-one correspondence between finitely generated torsion modules and pairs (V, L), where V is finite-dimensional.*

Proof. Observe that the direct sum of modules corresponds to the direct sum of vector subspaces. Hence if M is a finitely generated torsion $\mathbb{C}[t]$-module, using that $\mathbb{C}[t]$ is a principle ideal domain (since it's a Euclidean domain) we can invoke the Structure Theorem to write:

$$M \cong \bigoplus_{i=1}^{n} \mathbb{C}[t]/\langle f_i \rangle$$

where $f_i \neq 0$. Each summand is also a $\mathbb{C}$-module, and has dimension $\deg(f_i)$, which is finite for each i. Therefore the dimension of the direct sum is finite, and the vector space given by M is finite-dimensional (the associated linear map acts by right-multiplication by t in the quotient on each summand).

For the other direction, consider a pair (V, L), where $\dim V = N$. We wish to show that $(V, +, *)$ is finitely generated and torsion. The first is immediate, take any basis, and observe that it generates V as a $\mathbb{C}$-module, hence as a $\mathbb{C}[t]$-module.

The second is a small amount of interpretation. To show that $(V, +, *)$ is torsion, since V as a $\mathbb{C}$-module is a domain, then the determining factor is multiplication by t; i.e., applying $f(L)$. Indeed, for any $\mathbf{v} \in V$, observe the set $\{L^i \mathbf{v}\}_{i=0}^N$ is linearly dependent, hence there is a nontrivial linear combination:

$$\sum_{i=0}^{N} \alpha_i L^i \mathbf{v} = \mathbf{0}$$

Then if $f = \sum_{i=0}^N = \alpha_i x^i$, it follows that $f(L)\mathbf{v} = \mathbf{0}$, hence $f\mathbf{v} = \mathbf{0}$ when considering V as a $\mathbb{C}[t]$-module. Thus V corresponds to a finitely-generated torsion module. $\square$

Neat! This theory also gives a better idea of what is "going on behind the curtain" for the Jordan normal form.

Much Nicer Proof of Jordan Normal Form. Consider a linear map L on a finite-dimensional vector space V. By Theorem 37, this induces a finitely generated torsion $\mathbb{C}[t]$-module M. By the proof of the Structure Theorem, we can write:

$$M = \bigoplus_{i=1}^{N} \mathbb{C}[t] / \langle p_i(t)^{\alpha_i} \rangle$$

uniquely. We can do one better: since $\mathbb{C}[t]$ is an algebraically closed UFD, its primes are its irreducibles, which are linear functions. Thus there exist a set of values $\{\lambda_i\}_{i=1}^N$ (look familiar?) so that the above decomposition is written:

$$M = \bigoplus_{i=1}^{N} \mathbb{C}[t] / \langle (t - \lambda_i)^{\alpha_i} \rangle$$

The submodule $\mathbb{C}[t] / \langle (t - \lambda_i)^{\alpha_i} \rangle$ has as a basis:

$$\begin{cases} \mathbf{v}_1 = (t - \lambda_i)^{\alpha_i - 1} \\ \vdots \\ \mathbf{v}_{\alpha_i} = 1 \end{cases}$$

After all, this set is linearly independent, and its size matches the dimension. However, in this basis left-multiplication by $(t - \lambda_i)$ corresponds in the bijection to sending one basis element to the next, hence the corresponding linear map is of the form:

$$\begin{bmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ & & & & 0 \end{bmatrix}$$

Thus after pulling back to (V, L), it follows that $L - \lambda I$ is of the above form on the ith summand, hence L is of the form:

$$\begin{bmatrix} \lambda_i & 1 & & & \\ & \lambda_i & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda_i & 1 \\ & & & & \lambda_i \end{bmatrix}$$

on that summand. Hence in the direct sum of the bases we derived, L is written as a direct sum of Jordan blocks, and we get uniqueness for free from the proof of the Structure Theorem. □

Pretty slick. Here's another gorgeous corollary: last semester, Professor Borisov presented an elementary proof of the fact that any finite subgroup of F^* for a field F is cyclic. This had a few moving parts, and amounted to some number theory. That said, it didn't really show what was "going on," and now we have the tools to do so. As it turns out, all we need is the nuclear bomb that is the Structure Theorem, and some elementary counting!

Theorem 38. *Every finite subgroup of the multiplicative group of a field is cyclic.*

Proof. Let G be a finite subgroup of the multiplicative group of a field F. Since G is finite, it is both finitely generated and torsion, hence:

$$G = \bigoplus_{i=1}^{N} \mathbb{Z}/a_i\mathbb{Z}$$

where $1 \neq a_1|a_2|\dots|a_N \neq 0$. Finishing the proof amounts to demonstrating that $N = 1$.

Suppose for contradiction that some finite $H \leq F^*$ is written $\mathbb{Z}/a_1\mathbb{Z} \oplus \mathbb{Z}/a_2\mathbb{Z}$, where $1 \neq a_1|a_2 \neq 0$. Since $F[t]$ is a Euclidean domain, induction easily gives that $x^d - 1 = 0$ has at most d solutions in F. Every element of G is of the form $([i]_{a_1}, [j]_{a_2})$, and we have a_1 choices of i to be sent to 0 by raising to the a_1th power (i.e., multiplying by a_1 in a multiplicative group). But since $a_1|a_2$, and $a_2 \neq 0$, we can select at least a_1 elements which are also annihilated by a_1; since a_2/a_1 is an integer, select $j \in \{a_2/a_1 k : k \in [a_1]\}$, and observe that after raising to the a_1th power, this becomes $[a_2 k]_{a_2} = 1$. Thus there are a_1^2 solutions, and since $a_1 \neq 1$, this is impossible– the contradiction we sought. □

4.7 3/23/22: The Tensor Product: Definition and Elementary Theory

We have a direct sum of vector spaces, which (taken as an exterior direct sum) extends the notion of the disjoint union of sets. After all, if $|A| = n$ and $|B| = m$, then $|A \sqcup B| = n+m$, and if $\dim V = v$ and $\dim W = w$, then $\dim(V \oplus W) = v+w$. However, this begs a question: if the direct sum results in a multiple-coordinate vector, then what is left to correspond to the cartesian product of sets?

The way we extend this notion is via the tensor product (to be defined!), which transfers notions of linearity, which are preserved under sum but not product, to notions of bilinearity, which is the best generalization of a product we have.

Suppose V and W are vector spaces over a field $\mathbb{K}$. We define the **$\mathbb{K}$-tensor product of V and W** as:

$$V \otimes_{\mathbb{K}} W = \left\{ \sum_{i=1}^{N} \alpha_i(\mathbf{v}_i, \mathbf{w}_i) : \mathbf{v}_i \in V, _i \in W, \alpha_i \in \mathbb{K} \right\} / R$$

where R is the set of relations given by, for all $\lambda \in \mathbb{K}$, $\mathbf{v} \in V$, and $\mathbf{w} \in W$:

$$\begin{cases} \lambda(\mathbf{v}, \mathbf{w}) - (\lambda\mathbf{v}, \mathbf{w}) \\ \lambda(\mathbf{v}, \mathbf{w}) - (\mathbf{v}, \lambda\mathbf{w}) \\ (\mathbf{v}_1 + \mathbf{v}_2, \mathbf{w}) - ((\mathbf{v}_1, \mathbf{w}) + (\mathbf{v}_2, \mathbf{w})) \\ (\mathbf{v}, \mathbf{w}_1 + \mathbf{w}_2) - ((\mathbf{v}, \mathbf{w}_1) + (\mathbf{v}, \mathbf{w}_2)) \end{cases}$$

We can write the set we quotient as $\text{Free}(V \times W)$; the free module generated by the cartesian product of V and W.

Moving forward, we will be brave and write $V \otimes W$ when $\mathbb{K}$ is clear. Moreover, we introduce the following notation:

$$\mathbf{v} \otimes \mathbf{w} = [(\mathbf{v}, \mathbf{w})] \in V \otimes W$$

This definition is *ugly*. When you have a hammer, everything is a nail: we have freedom to specify all sorts of modules by quotienting out relations, but that doesn't mean it's the best route! In particular, this space which we squish and squeeze to force $\otimes$ to be bilinear is characterized by:

Theorem 39 (Universal Property of the Tensor Product)**.** *Suppose that $f : V \times W \to U$ is bilinear. Then there exists a unique linear map $\pi : V \otimes W \to U$ so that $f = \pi \circ \otimes$.*

Proof. Given a free module M, we can easily form a correspondence between linear maps on M and set maps on a basis of M. Indeed, just extend it by linearity.

Thus define $F : \text{Free}(V \times W) \to U$ by $F(\mathbf{v}, \mathbf{w}) = f(\mathbf{v}, \mathbf{w})$, and extend it linearly so that:

$$F\left(\sum a_i(\mathbf{v}_i, \mathbf{w}_i)\right) = \sum a_i f(\mathbf{v}_i, \mathbf{w}_i)$$

Because f is bilinear, F vanishes on each relational expression in R, hence F descends to a linear map of the quotient $\pi : V \otimes W = \text{Free}(V \times W)/R \to U$ so that $\pi(v \otimes w) = F(v, w) = f(v, w)$. Thus such a π exists.

Uniqueness follows from the unique definition of f.

□

That π is unique allows us to redefine the tensor product of V and W as the unique vector space Z so that every bilinear map factors through Z linearly.

The universal property is useful for many other reasons; in particular, we can use it to find a basis for $V \otimes W$.

Theorem 40. *Suppose $\mathscr{B}_V = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a basis of V, and $\mathscr{B}_W = \{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$ is a basis of W. Then $\{\mathbf{v}_i \otimes \mathbf{w}_j\}_{i \in [n], j \in [m]}$ is a basis of $V \otimes W$.*

Proof. Let $\mathbf{v} \in V$ and $\mathbf{w} \in W$. Then $\mathbf{v} = \sum_i a_i \mathbf{v}_i$ and $\mathbf{w} = \sum_j b_j \mathbf{w}_j$, hence $\mathbf{v} \otimes \mathbf{w} = \sum_{i,j} a_i b_j (\mathbf{v}_i \otimes \mathbf{w}_j)$.

To see uniqueness, fix i and j and define a bilinear map:

$$F_{ij}(\mathbf{v}, \mathbf{w}) = \left([\mathbf{v}]_{\mathscr{B}_V}\right)_i \left([\mathbf{w}]_{\mathscr{B}_W}\right)_j$$

where $[-]_C$ is the basis representation of $-$ in C. F_{ij}'s bilinearity is an easy corollary of the bilinearity of multiplication.

By the Universal Property of the Tensor Product, there is a unique linear map $\pi_{ij} : V \times W \to \mathbb{K}$ so that $F_{ij} = \pi_{ij} \circ \otimes$. We can apply π_{ij} to the elements of our (purported) basis to see:

$$\pi_{ij}(\mathbf{v}_n \otimes \mathbf{w}_m) = \begin{cases} 1 & \text{if } i = n, j = m \\ 0 & \text{else} \end{cases}$$

Now suppose that we have a linear combination:

$$\mathbf{0} = \sum_{ij} a_{ij} (\mathbf{v}_i \otimes \mathbf{w}_j)$$

Since we can always write $\mathbf{0} = \sum_{ij} 0(\mathbf{v}_i \otimes \mathbf{w}_j)$, it follows that $\pi_{nm}(\mathbf{0}) = 0$. Applying π_{nm} to both sides:

$$0 = \sum_{ij} a_{ij} \pi_{nm}(\mathbf{v}_i \otimes \mathbf{w}_j) = a_{nm}(\mathbf{v}_n \otimes \mathbf{w}_m)$$

hence all coefficients of the linear combination are 0, thus $\{\mathbf{v}_i \otimes \mathbf{w}_j\}$ is linearly independent. □

Corollary 13. *If $\dim(V) = n$ and $\dim(W) = m$, then $\dim(V \otimes W) = nm$.*

We now have a set of powerful tools to understand the tensor product: an explicit basis, a relation between $\hom(V \otimes W, U)$ and bilinear maps $V \times W \to U$, and an explicit set of quotienting relations. This is enough for the moment; now we will look at other vector spaces, and their relation to the tensor product.

Suppose V is a vector space over $\mathbb{K}$. We say that $V^* = \hom(V, \mathbb{K}) = \{f : V \to \mathbb{K} : f \text{ is linear}\}$ is V's **dual vector space**. Elements of V^* are called **covectors**. In general, we can get a canonical isomorphism between finite-dimensional vector spaces V and their dual V^* if we have a non-degenerate bilinear form f on V; for all $\alpha \in V^*$, there is a unique $\mathbf{u} \in V$ so that for all $\mathbf{v} \in V$, $\alpha(\mathbf{v}) = f(\mathbf{u}, \mathbf{v})$.

If V has a basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, we can use this isomorphism to find its **dual basis**. The most basic bilinear form is the dot product; indeed, if V has the dot product, then we get a dual basis:

$$\alpha_i(\mathbf{v}_j) = \delta_{ij}$$

Here are two ways that the tensor product interacts with this construction: the space of bilinear functions from V^2 to $\mathbb{K}$ is just $(V \otimes V)^* \cong V^* \otimes V^*$. We can also identify $\hom(V, W) \cong V^* \otimes W$.

4.8 3/25/22: The General Tensor Product: Various Constructions

The tensor product works equally well for M over a CRU R. Indeed, suppose that A is a CRU with unity, and M and N are A-modules. Then as in last section, define $M \otimes_A N = \text{Free}(M \times N)/R$, where R are the relations as in last section.

We get the same universal property:

Theorem 41. *Suppose that M, N, K are A-modules. For every biholomorphism $F : M \times N \to K$, there exists a unique homomorphism $\alpha : M \otimes_A N \to K$ such that $F = \alpha \circ \otimes$.*

The proof is exactly the same as that of Theorem 39.

We can see a little of how the module tensor product works by examining $A = \mathbb{Z}$. Indeed, one can verify that $\mathbb{Z}^m \otimes_{\mathbb{Z}} \mathbb{Z}^n = \mathbb{Z}^{nm}$, and interestingly enough, $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/\gcd(n,m)\mathbb{Z}$. We will prove the case that $\gcd(n,m) = 1$.

Proof. To see this, observe that $m([1]_m \otimes [1]_n) = 0$, and $n([1]_m \otimes [1]_n) = 0$. Since $\gcd(n,m) = 1$, there are u and v such that $nu + mv = 1$. Hence for all $a \in \mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$,

$$\begin{aligned} a = 1a &= (nu + mv)a \\ &= (nu + mv)(\alpha[1]_m \otimes \beta[1]_n) \\ &= 0 \end{aligned}$$

□

Next, we will discuss various constructions relating to the tensor product and algebraic objects.

If A, B are rings and $\pi : A \to B$ is a ring homomorphism, then we can view B as an A-module with the multiplication $a \cdot b = \pi(a)b$. Hence for every A-module M, we can see $M \otimes_A B$ as an A-module, and we can even do more; if $z = \sum a_i(m_i \otimes b_i)$, define:

$$z * b = \sum a_i(m_i \otimes b_i b)$$

To actually verify $(M *_A B, +, *)$ as a B-module, we need to verify that the scalar multiplication is bilinear on $M \times B$ (hence descends uniquely into $M \otimes_A B$), and satisfies the module axioms. Both of these are true, and we will not show them— they amount to checking.

In fact, we can incorporate these constructions to show the following; if A is a CRU with unity, and B and C are rings so that there are ring homomorphism $\pi : A \to B$ and $\tau : A \to C$. Then we can find operations which make $B \otimes_A C$:

1. An A-module, given by the first operation above,
2. a B-module, given by the second operation above,
3. a C-module, given by the second operation above,

4. and a ring, given by $(a \otimes b)(c \otimes d) = ac \otimes bd$ (extended linearly).

Here are two examples.

1. If $A = \mathbb{Z}$, $B = \mathbb{Q}$, and M is a finitely generated $\mathbb{Z}$-module, then $M \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}^r$ as a $\mathbb{Q}$-module (i.e., as the third item above). Indeed:

$$M \otimes_{\mathbb{Z}} \mathbb{Q} \cong (\mathrm{Tor}(M) \otimes_{\mathbb{Z}} \mathbb{Q}) \oplus (\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q})^r$$

   So we need only show that the left summand is $\{0\}$, and the right $\mathbb{Q}^r$. For the first, let $x \otimes q \in \mathrm{Tor}(M) \otimes \mathbb{Q}$. Then there is some $k \in \mathbb{Z}$ such that $kx = 0$. Then $x \otimes q = x \otimes (k(q/k)) = kx \otimes q/k = 0$.

   We can see that every element of $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$ is a linear combination with $\mathbb{Z}$ coefficients $n \otimes q \in \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$. Then $n \otimes q = n(1 \otimes q)$, and after identifying $(1 \otimes q)$ with q, we see that the multiplication $(1 \otimes q)q' = 1 \otimes qq'$ gives the module structure we desire.

2. If $A = \mathbb{Q}$ and $B = \mathbb{Q}[3^{1/3}] \cong \mathbb{Q}[x]/\langle x^3 - 2\rangle$, and $C = \mathbb{R}$, where the relevant homomorphisms are the inclusions, then we claim:

$$B \otimes_A C = \frac{\mathbb{Q}[x]}{\langle x^3 - 2\rangle} \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}[x]/\langle x^3 - 2\rangle \cong \frac{\mathbb{R}[x]}{\langle x - 3^{1/3}\rangle} \oplus \frac{\langle \mathbb{R}[x]\rangle}{\langle x^2 + 2^{1/3}x + 2^{2/3}\rangle}$$

   The second isomorphism follows from the Chinese Remainder Theorem, so we need only show the first.

   Indeed, if we send:

$$(a[1] + b[x] + c[x^2]) \otimes r \mapsto ra[1] + rb[x] + rc[x^2]$$

   then the operation in the third item above gives that this is a homomorphism, hence an isomorphism. This kind of tensor product is called a **base change**, where if two fields $A \subset C$ and B is an A-algebra (an A-module with a compatible ring structure), then $B \otimes_A C$ is the according C-algebra.

4.9 3/30/22: The Localization of a Module

In this section, we will discuss an interesting construction (which we have seen before), then generalize it to modules and discuss one or two attributes.

We will not delve deep into the theory of localizations; for our purposes, this is a construction which produces more examples of rings and modules, but as we will see, the object is a natural one, and crops up in many other places that we will not discuss.

Recall from the previous course that we can form $\mathbb{Q}$ from $\mathbb{Z}$ by considering the set $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/\sim$, where $(n, m) \sim (x, y)$ if and only if $ny - mx = 0$. We will discuss various generalizations.

The first is the most straightforward: if R is a domain, we can construct the **field of fractions** $Q(R)$ in the same fashion; observe that $R \hookrightarrow Q(R)$ (via identification with constants) is an embedding.

The next is more general; we let R be any CRU, and select any multiplicative system $S \subseteq R$ to form the **localization of R with respect to S**, given by:

$$R_S = (R \times S)/\sim$$

where $(x_1, s_1) \sim (x_2, s_2)$ if and only if there is some $s_3 \in S$ so that $s_3(s_2x_1 - s_1x_2) = 0$. To see that this is an equivalence relation, observe:

- The s which certifies reflexivity is 1.
- Given an s which certifies $(x_1, s_1) \sim (x_2, s_2)$, the certification of the symmetrical relation is $-s$.
- Given s' and s'' that certify $(x_1, s_1) \sim (x_2, s_2)$ and $(x_2, s_2) \sim (x_3, s_3)$, respectively, the certification of the transitive relation is $s_2s's''$ (multiply the first relation by $s_3s's''$, the second by $s_1s's''$, and add).

We write $[(a, b)]$ as a/b, and on the localization we define the obvious operations:

$$\frac{x_1}{s_1}\frac{x_2}{s_2} = \frac{x_1x_2}{s_1s_2}$$

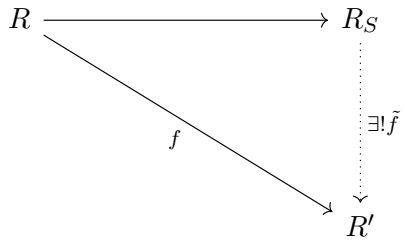
$$\frac{x_1}{s_1} + \frac{x_2}{s_2} = \frac{s_2x_1 + s_1x_2}{s_1s_2}$$

These are in fact well-defined; it is enough to check for one operand, and that is not very difficult.

Now that we can lift up to the level of operations, it is a further check that R_S is a CRU, and just like the field of fractions, we get a homomorphism $h : R \to R_S$ by $r \mapsto r/1$; however, this is not necessarily an embedding. In fact, $\ker(h) = \{r \in R : \exists s \in S \text{ s.t. } rs = 0\}$, the set of S-zero-divisors in R.

Not unlike the tensor product, this space is much more natural than is obvious from the definition. Indeed, we may specify R_S by one of the best things we could ever get: a universal property!

Theorem 42 (Universal Property of the Localization)**.** *If $f : R \to R'$ is a homomorphism so that for all $s \in S$, $f(s)$ is invertible in R', then there exists a unique map $\tilde{f} : R_S \to R$ so that the following diagram commutes:*



We will not be proving this, but it is worth mentioning to indicate how *pervasive* a localization is.

Here are some examples of multiplicative systems that are commonly used:

1. If R is a domain, then $R \setminus \{0\}$ is a multiplicative system. This produces the field of fractions.

2. If P is a prime ideal in R, let $S = R \setminus P$. That S is multiplicative follows from primacy of P, and we often denote this localization as R_P.

3. If $f \in R$, we can take the set $\{1, f, f^2, \dots\}$ as S. Often, this localization is denoted R_f.

The third way we can generalize this extends the localization of a ring to a module; if M is an R-module (with multiplication $\cdot$), and S a multiplicative system in R, then we can define an R_S-module:

$$M_S = (M \oplus S)/\sim$$

where $(m_1, s_1) \sim (m_2, s_2)$ if and only if there is some $s_3 \in S$ so that $s_3 \cdot (s_2 \cdot m_1 - s_1 \cdot m_2) = 0$. The same proof as before shows that $\sim$ is indeed an equivalence relation. We also define the appropriate operations:

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}$$

$$\frac{x}{s_1} \cdot \frac{m}{s_2} = \frac{x \cdot m}{s_1 s_2}$$

but since one operand is in R and other other is in M, we would have to check well-definition separately. This is tedious, so we won't. The next result is a similar level of difficulty (so we won't prove it), but is significant in unifying the notion of the tensor product and the localization:

Theorem 43. *Suppose M is an R-module, and S is a multiplicative system in R. Then:*

$$M_S \cong M \otimes_R R_S$$

when the right-hand side is considered as an R_S-module. The identification is given by:

$$\frac{xm}{s} \longleftrightarrow m \otimes \frac{x}{s}$$

[An aside: I haven't really thought about this, but I suspect this is *not* tedious! We should be able to leverage Theorem 41 and 42 to get a pretty slick proof... I think?]

As a foil to the elegance of this identification, it is worth noting that the general tensor product over a nonlocalized ring is *not* as nice in general. One way of seeing this is that the localization functor is exact; if:

$$0 \to N \to M \to K \to 0$$

is short exact, then:

$$0 \to N_S \to M_S \to K_S \to 0$$

is short exact. On the other hand, for a general tensor product we only obtain that:

$$N \otimes_R L \to M \otimes_R L \to K \otimes_R L \to 0$$

is short exact; we lose the first map as part of exactness.

Chapter 5

Elementary Field Theory

5.1 4/1/22: A Review of Rudimentary Field Theory

A commutative ring with unity F is called a **field** if for every $x \neq 0$ there is some $y \in F$ so that $xy = 1$. Such a y is always unique. Field theory asks different questions than non-field ring theory, much of which can be attributed to the following fact:

Lemma 25. *A field K has only two ideals: $\{0\}$ and K itself.*

Proof. Suppose $I \subseteq K$ is an ideal of K. If $I = \{0\}$, we are done, so suppose not. Then there is some $i \neq 0 \in I$, hence by closure under multiplication, $ii^{-1} = 1 \in I$, so $I = K$. □

Algebraic structures have fundamental relations with maps from their superstructure, and this case is no different:

Corollary 14. *Suppose K_1 and K_2 are fields, and $f : K_1 \to K_2$ is a ring homomorphism that sends 1_{K_1} to 1_{K_2}. Then f is injective.*

Proof. By the premise, $1_{K_1} \notin \ker(f)$, so by Lemma 25 $\ker(f) = \{0\}$. □

Thus the weighty restriction of only two ideals has as its morphism-analog the fact that the only field homomorphisms to consider are the zero map, and inclusions.

However, it turns out that inclusions are *vital* to field theory. Indeed, seeing a field inside another is the route to follow: if K_1 and K_2 are fields so that $K_1 \subset K_2$, we say that K_2 is a **field extension** of K_1. The classic example is the chain of field extensions $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

This innocuous notion will form the cornerstone of the theory. Before moving forward, some examples (which will also implicitly establish some notation):

1. $\mathbb{Q}$, the rational numbers. Each $0 \neq q \in \mathbb{Q}$ has inverse $1/q$.
2. $\mathbb{R}$, the real numbers. Each $0 \neq r \in \mathbb{R}$ has inverse $1/r$.
3. $\mathbb{C}$, the complex numbers. Each $0 \neq c = a + bi \in \mathbb{C}$ has inverse $1/c = (a - bi)/|c|^2$.
4. $\mathbb{Q}(x)$, the field of rational functions with rational coefficients:

$$\left\{ \frac{p(x)}{q(x)} : p \in \mathbb{Q}[x], q \in \mathbb{Q}[x] \setminus \{0\} \right\}$$

   Each $p \in \mathbb{Q}(x)$ has inverse $1/p$.

5. The **field of fractions** $D(x)$ of an integral domain D, constructed as in the prequel. Observe that $\mathbb{Q}[x]$ is an integral domain, hence in the most literal notation $\mathbb{Q}(x) = \mathbb{Q}[x](x)$.

   Generally speaking, $(D(x))(y) \cong D(x, y)$ via simplification of fractions, and in fact $K(x, y)$ is the field of fractions of the ring $K[x, y]$

6. $\mathbb{Q}[x]/\left\langle x^3-2\right\rangle$, the quotient field formed by the ideal $\left\langle x^3-2\right\rangle$. How do we know that this is a field? Observe that by $p(x)=x^3-2$ is irreducible. Since $\mathbb{Q}[x]$ is a UFD, all irreducible elements are prime (this is not generally true), hence p is prime in $\mathbb{Q}[x]$. Since $\mathbb{Q}[x]$ is a PID, $\langle p\rangle$ is a prime ideal (this is not generally true; the converse is what is true in any domain), hence again by PID $\langle p\rangle$ is maximal.

   We can also give a specific argument (which serves as a template for the one above); the paragraph above utilized some heavy weaponry.

   Proof. Let f be irreducible in $\mathbb{Q}[x]$. We wish to show that for every nonzero $[g(x)]\in\mathbb{Q}[x]/\langle f\rangle$, there is some $[h(x)]$ so that $[g(x)][h(x)]=[1]$; i.e., that $gh(x)\equiv 1 \pmod f$. Consider the ideal $\langle g,f\rangle=\langle f_1\rangle$. Observe that f does not divide g, since $[g]\neq[0]$, hence $f_1=1$ by irreducibility. Thus $\langle f_1\rangle=\mathbb{Q}[x]$, finishing the proof. □

We will be dealing a lot with quotient fields of this form, so it is worthwhile to have an explicit analysis of one. We now know that $F=\mathbb{Q}[x]/\left\langle x^3-2\right\rangle$ is a field, but we should check what form its elements take. The lowest degree representative of each element of such a quotient is at most degree 2, hence $a\in F$ is of the form $[a_0+a_1x+a_2x^2]$. If the triplet of coefficients of two elements are distinct, then they are as well; if $a\neq b$ but $(a_0,a_1,a_2)=(b_0,b_1,b_2)$, then:

$$[a-b]=[(a_0-b_0)]+[(a_1-b_1)][x]+[(a_2-b_2)][x^2]=[0]=[p(x)h(x)]$$

If $h=0$, then their difference would have degree 3, which is impossible. If $h\neq 0$, then:

$$2\geqslant \deg(fh)=\deg f+\deg h\geqslant 3$$

[This line of reasoning confused me]

We can also construct a multiplication table:

$\cdot$	1	x	x^2
1	1	x	x^2
x	x	x^2	2
x^2	x^2	2	$2x$

Moreover, $\mathbb{Q}$ naturally embeds into $\mathbb{Q}[x]$, and as each element is sent to a constant (which is unaffected by the quotient), we can push the embedding through the projection $\mathbb{Q}[x]\to F$ to embed $\mathbb{Q}$ into the quotient ring.

It then follows that F is a vector space over $\mathbb{Q}$, and it is not too hard to see that in this case a basis is $\{[1],[x],[x^2]\}$; more generally, $\dim_{\mathbb{Q}}(F)=\deg(p)$.

It also follows that F is a field extension of $\mathbb{Q}$, and we can write $\mathbb{Q}[x]/\langle p\rangle$ as $\mathbb{Q}[a]=\{q+pa : q,p\in\mathbb{Q}\}$ for some a a root of p.

In the above example, $\mathbb{Q}[x]/\left\langle x^3-2\right\rangle\cong\mathbb{Q}[2^{1/3}]$.

The field $\mathbb{Q}(x)$ can also be thought of as a field extension, since $\mathbb{Q} \hookrightarrow \mathbb{Q}(x)$, but we call this one a **transcendental field extension**, forming an infinite-dimensional vector space over $\mathbb{Q}$. It is worth noting that $\mathbb{Q}(x) \cong \mathbb{Q}(\pi)$ via the substitution map, which should motivate the notation. The real reason for the notation comes from the following branch of theory.

Suppose L extends F. Then an element $a \in L$ is **algebraic** over F if there is some $0 \neq f(x) \in F[x]$ so that $f(a) =_L 0$. If there is no such f, we will call a **transcendental** over F. We will discover that all extensions by algebraic numbers have finite dimension as a vector space over the base field. Thus as algebraic extension have finite dimension, it makes sense to name infinite-dimensional extensions transcendental. We will explore this theory more next section.

Moving on, if a is algebraic over F, we know there is a polynomial which is zero on a with coefficients in F. The **minimal polynomial** is the unique monic polynomial which has a as a root, coefficients in F, and has minimal degree with respect to this property.

That $\mathbb{Q}[2^{1/3}] \cong \mathbb{Q}[x]/\left\langle x^3 - 2 \right\rangle$ should indicate the fact that the map $F[x] \to L$ given by $p(x) \mapsto p(a)$ is a ring homomorphism, as we can surject $\mathbb{Q}[x]$ onto $\mathbb{Q}[x]/\left\langle \text{minpoly}(a) \right\rangle \cong \mathbb{Q}[a]$ (we have not yet proved this isomorphism).

An alternative perspective is to prove that this is a homomorphism directly, and then see that $\ker(f)$ is just $\langle \text{minpoly}(a) \rangle$.

Before next section, a vital lemma:

Lemma 26. $\text{minpoly}(a)$ *is irreducible in* $F[x]$

This follows from the division algorithm; if $\text{minpoly}(a)$ is written hg, then exactly one has a as a root (or we contradict minimality), hence g is a constant.

To conclude this set of miscellany in fundamental field theory, we will address the question: are there real numbers transcendental over $\mathbb{Q}$? Certainly we have a definition for such numbers, but it's possible the set which it indexes is null for some fields, and one of the simpler fields is $\mathbb{Q}$. We know from folklore that numbers like π and e are transcendental, we actually know very few numbers to concretely be transcendental. However, we give a construction to find one through elementary methods.

Theorem 44. *The number* $\alpha = \sum \frac{1}{2^{n!}}$ *is transcendental over* $\mathbb{Q}$.

Proof. Certainly the sum converges, so α exists. Suppose for contradiction it is not; then let $f(x) = \text{minpoly}_{\mathbb{Q}}(\alpha)$ of degree d. Pick D so that $Df(x) \in \mathbb{Z}[x]$.

Define σ_N to be α's Nth partial sum; hence $\sigma_N \to \alpha$ as $N \to \infty$. Moreover, let $x_N = f(\sigma_N)$. As α is clearly not rational, and f is irreducible of degree > 1, it follows that f has no rational root. Since $\sigma_N \neq \alpha$, it follows that $x_N \neq 0$. Since $x_N \neq 0$, it follows that:

$$|(2^{N!})^d D x_N| \geqslant 1$$

The fundamental theorem of algebra gives that $f(x) = \prod_{i=1}^{d}(x - \alpha_i)$, where $\alpha_i \in \mathbb{C}$ and we let $\alpha_1 = \alpha$. Hence:

$$|x_N| = \prod_{i=1}^{d} |\sigma_N - \alpha_1| \leqslant |\sigma_N - \alpha_1|(\sigma_N + M)^{d-1}$$

for $M = \max_{i \neq 1}\{1, |\alpha_i|\}$. This is sufficient to find a contradiction. We can estimate the first factor of the right-hand side, then use that to alter the estimate of $|x_N|$, squeezing it from above by an expression which tends to zero, contradicting our lower bound on it.

Indeed:

$$|\sigma_N - \alpha_1| = \sum_{n=N+1}^{\infty} \frac{1}{2^{n!}} \leqslant \frac{1}{2^{(N+1)!}} \left(\sum_{n=0}^{\infty} \frac{1}{2^n} \right) = \frac{2}{2^{(N+1)!}}$$

Therefore:

$$|x_N| \leqslant \frac{2}{2^{(N+1)!}} (\sigma_N + M)^{d-1}$$

And so, using the estimate above:

$$1 \leqslant |(2^{N!}) D x_N| \leqslant 2 \frac{2^{d(N!)} D}{2^{(N+1)!}} (\sigma_N + M)^{d-1}$$

However, taking the limit as $N \to \infty$ gives $1 \leqslant 0$, which is a contradiction.

□

5.2 4/4/22: More Rudimentary Field Theory

We continue to tour the theory, picking up significant insights along the way.

First, a hugely important result (with an easy proof!):

Theorem 45. *Suppose $K \subset L$ is a field extension, and $a \in L$ is algebraic over K, with K-minimal polynomial f. Then:*

$$K[a] \cong K[x]/\langle f \rangle$$

Proof. The kernel of the substitution map $f(x) = f(a)$ is, by definition, generated by f. Hence its image, $K[a]$, is isomorphic to $K[x]/\langle f \rangle$. □

Hence a basis of $K[a]$ as a vector space over K is nothing but $\{a^i : 0 \leqslant i < \deg(f)\}$. This implies that $\dim_K(K[a]) = \deg(f)$; this is a notable invariant called the **degree** of the field extension, and we write it as $[K[a] : K]$ (more generally, $[L : K]$). We call an extension $K \subseteq L$ **finite** if $[L : K]$ is finite.

For our next result, there is a second notion of "finiteness" to consider; we say a field extension $K \subset L$ is **finitely K-generated** if there are $a_1, \ldots, a_n \in L$ so that every $a \in L$ can be written as a quotient $p(a_1, \ldots, a_n)/q(a_1, \ldots, a_N)$ for $p, q \in K[x_1, \ldots, x_n]$. This will be useful for the following technical result, but many of the fields we consider will be easily seen to be finitely generated.

Last, we say a field extension $K \subset L$ is **algebraic** if every $a \in L$ is algebraic over K. We can capture the relation between these three notions as follows:

Theorem 46. *A field extension $K \subset L$ is finite if and only if it is both finitely generated and algebraic.*

This is not so implausible; algebricity entails a polynomial of finite degree for each element of the extension, and finite-generation gives that we only have finitely-many such elements; hence a finite "total degree" of the extension.

To show Theorem 46, we will first prove a result of linear algebra which has a significant implication, then a theorem of pure field theory, then a lemma which is *stronger* than the reverse direction.

Theorem 47. *Suppose $K \subset L \subset F$. Then $\dim_K(L) \dim_L(F) = \dim_K(F)$.*

Proof. Suppose that $\{a_1, \ldots, a_n\}$ is a basis of L over K, and $\{b_1, \ldots, b_m\}$ is a basis of F over L. We will prove that: $\mathscr{B} = \{a_i b_j\}_{i \in [n], j \in [m]}$ is a basis of F over K.

We first prove B spans F. Suppose $x \in F$. Then we can write x as a linear combination of the b_j with coefficients in L: $x = \sum_{j=1}^m l_j b_j$.

Since the a_i are a basis of L over K, it follows that $l_j = \sum_{i=1}^n k_{ij} a_i$, where $k_{ij} \in K$. Thus $x = \sum_{i=1}^n \sum_{j=1}^m y_{ij} a_i b_j$, so $\mathscr{B}$ spans F over K.

Now we show that $\mathscr{B}$ is linearly independent. Suppose that $\sum_{i,j} c_{ij}(a_i b_j) = 0$. It suffices to show that $c_{ij} = 0$ for all i, j. Indeed, we rewrite the combination as $\sum_{j=1}^m \left(\sum_{i=1}^n c_{ij} a_i\right) b_j = 0$

Using that the b_j are a basis for F over L, for each j, $\sum_{i=1}^n c_{ij} a_i = 0$. Since the a_i are a basis for L over K, for each j and each i the $c_{ij} = 0$, completing the proof. □

Corollary 15 (Multiplicativity of the Degree)**.** *Suppose $K \subset L \subset F$. Then:*

$$[F : L][L : K] = [F : K]$$

You don't want to forget this one!

Next, a theorem which is generally useful.

Theorem 48. *Suppose $K \subset L$ is algebraic. Then if R is a ring so that $K \subset R \subset L$, it is in fact a field.*

We will provide two proofs!

Proof 1. Suppose $K \subset R \subset L$, and let $r \in R$. Then by algebricity, r has a minimal polynomial in $K[x]$ which is irreducible in $K[x]$. By the reasoning discussed on page 87 (item 6), and Theorem 45, it follows that $K[r]$ is a field, hence $r^{-1} \in K[r]$. The theorem follows from observing that $K \subset K[r] \subset R$. □

Proof 2. By algebricity, r has a K-minimal polynomial $\sum k_i x^i$. Then $\sum_{i \neq 0} k_i r^i + k_0 = 0$, so $1 = \left(-\frac{1}{k_0} \sum_{i \neq 0} k_i r^{i-1}\right) r$. □

Each proof has their appeal; the first uses some heavy machinery to strike at the heart of the matter, while the second gives an explicit computation.

Observe that Theorem 48 has an impact on notation; in an algebraic extension of K, there is no difference between $K[a_1, \ldots, a_n]$ and $K(a_1, \ldots, a_n)$. Thus we are free to switch notation as we wish.

Lemma 27. *Suppose $K \subset L$ is a field extension and L is K-generated by $\{a_1, \ldots, a_n\}$, where each a_i is algebraic over K. Then L is a finite extension of K.*

Proof. Consider the chain:

$$K \subset K(a_1) \subset \cdots \subset K(a_1, \ldots, a_n) = L$$

If we can show at each step that the extension is finite, we are done by multiplicativity of the degree. Indeed, we claim that $K(a_1, \ldots, a_i) \subset K(a_1, \ldots, a_{i+1})$ is finite. Since a_{i+1} is algebraic over K, it is certainly algebraic over $K(a_1, \ldots, a_i)$, so it has a $K(a_1, \ldots, a_i)$-minimal polynomial f, thus $[K(a_1, \ldots, a_{i+1}) : K(a_1, \ldots, a_i)]$ is finite; it is at most the degree of $\text{minpoly}_K(a_{i+1})$. □

Now we can prove Theorem 46.

Proof of Theorem 46. The backwards direction follows from Lemma 27.

To see the forward direction, suppose $K \subset L$ is a finite extension. Then we can find a K-basis $\{a_1, \ldots, a_n\}$ of L; but this basis K-generates L, so we get finite K-generation essentially for free. Thus the remaining difficulty is showing that $K \subset L$ is algebraic– but this is not so difficult.

Take some $a \in L$, and observe that the set $\{a^i : 0 \leqslant i \leqslant [L:K]\}$ has $([L:K]+1)$ elements, hence is linearly dependent over K. Thus there are $\alpha_i \in K$, at least one nonzero, so that $\sum_{i=1}^{[L:K]} \alpha_i a^i = 0$. Hence $f(x) = \sum_{i=1}^{[L:K]} \alpha_i x^i$ is in $K[x]$, and vanishes on a; therefore, a is algebraic over K. □

For most purposes, this is essentially a complete description of a finite extension. The qualitative upshot is that if we adjoin finitely many algebraic elements to a field, we are guaranteed that that extension is finite; alternatively, given a finite extension, we know that there are finitely many algebraic elements which distinguish it from the base field. The first qualitative observation has a quantitative analogue:

Theorem 49. *Suppose $K \subset L$ and L is K-generated by $\{a_1, \ldots, a_n\}$, each algebraic over K. If $\deg(\mathrm{minpoly}_K(a_i)) = d_i$, then:*

$$\mathrm{lcm}(d_i) \leqslant [L:K] \leqslant \prod_{i=1}^{n} d_i$$

Proof. Write $K = K_0$ and $K(a_1, \ldots, a_i) = K_i$, and observe that:

$$K_0 \subset K_1 \subset \cdots \subset K_n$$

Since each $K_i \supset K$, it holds that $[K_{i+1} : K_i] \leqslant d_i$; this follows from the observation that $\mathrm{minpoly}_{K_i}(a_{i+1}) | \mathrm{minpoly}_K(a_{i+1})$ in K_i. Multiplicativity of the degree gives the upper bound.

To see the lower bound, observe that the chain $K \subset K_i \subset L$ alongside multiplicativity of the degree yields that $[L:K] = [L:K_i]d_i$, hence for each i, the degree $[L:K]$ must be a multiple of d_i. Thus it must be at least the lcm of the d_j. □

Endemic to mathematics is the notion of a **closure system** (S, K), where S is a set and K are the **closed sets** of S; which can be defined as the cryptomorphic type of three equivalent representations:

1. We define a **closure operator** $\mathrm{cl} : 2^S \to K$ which satisfies three axioms for every $X, Y \subseteq S$:

   (a) $X \subseteq \mathrm{cl}(X)$,
   (b) $X \subseteq Y \implies \mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$, and
   (c) $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$

   We can define the closure of a set X as $\mathrm{cl}(X)$.

2. We can define the closure of a set X as $\bigcap_{\substack{C \in K \\ C \supseteq X}} C$.

3. We can define the closure of a set X as the result of applying arbitrarily many **closure rules**, which are of the form "if $Y \subseteq X$, then $\alpha(Y) \in X$."

Three examples are the topological closure in a metric space, the linear span, and the free group on a set.

With our discussion of algebraic extensions, we obtain another example: we say that a field L is **algebraically closed** if every nonconstant element of $L[x]$ vanishes somewhere in L. Given an extension $K \subset L$, we say that L is an **algebraic closure** if $K \subset L$ is algebraic, and L is algebraically closed.

The classic example is that $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. However, it is a bit less obvious what an algebraic closure looks like over any field; the next theorem contributes to a way of parsing such a question.

Theorem 50. *Suppose $K \subset L$ is an extension, and $a, b \in L$ are algebraic over K. Then $a + b$ and ab are algebraic over K.*

Proof. Consider the extension $K \subset K(a, b)$. By multiplicativity of the degree, $[K(a, b) : K] < \infty$, hence the extension is algebraic by Theorem 46. Evidently $a + b$ and ab are in $K(a, b)$, so they are algebraic over K. □

Theorem 50 amounts to saying that the set of elements of L algebraic over K form a ring, and by Theorem 48, they in fact form a field! Neat.

The next theorem says that algebricity of extensions is transitive, and that an algebraic extension can be split into two, if there is an intermediary field.

Theorem 51. *Suppose $K \subset F \subset L$ is a chain of field extensions. Then $K \subset L$ is algebraic if and only if $K \subset F$ and $F \subset L$ are both algebraic.*

Proof. Suppose $K \subset L$ is algebraic. We get algebricity of the intermediary extensions nearly for free; if $a \in F$, then $a \in L$, so $\text{minpoly}_K(a)$ is a K-polynomial which vanishes on a. If $l \in L$, then since $K \subset L$, $\text{minpoly}_K(a)$ is an F-polynomial which vanishes on a.

The other direction takes a little more work.

Suppose $K \subset F$ and $F \subset L$ are algebraic. Let $a \in L$; then there is some $0 \neq p = \sum q_i x^i \in F[x]$ so that $p(a) = 0$. Each q_i is algebraic over K, so the extension $K \subset K(q_0, \ldots, q_n)$ is finite, and since $p \in K(q_0, \ldots, q_n)[x]$, it holds that a is algebraic over $K(q_0, \ldots, q_n)$, hence the extension $K(q_0, \ldots, q_n) \subset K(q_0, \ldots, q_n, a)$ is finite, so by multiplicity of the degree, $K \subset K(q_0, \ldots, q_n, a)$ is finite hence algebraic: a is algebraic over K. □

Now we can describe a canonical algebraic closure, which turns out to be exactly what we expect!

Corollary 16. *Suppose $K \subset L$ is a field extension, where L is algebraically closed. Then*

$$F = \{l \in L : l \text{ is algebraic over } K\}$$

is an algebraic closure of K.

Proof. By Theorem 48, F is a field, and it is certainly algebraic over K. Thus it suffices to show algebraic closure.

Suppose $p \in F[x]$. Then $p \in L[x]$, so there is $a \in L$ so that $p(a) = 0$; write $p(x) = \sum c_i x^i$. Since each c_i is in F, it follows by definition that each is algebraic over K, so since a is algebraic over $K(c_0, \ldots, c_n)$, we apply Theorem 51 to the chain:

$$K \subset K(c_0, \ldots, c_n) \subset K(c_0, \ldots, c_n, a)$$

to conclude that a is algebraic over K, hence in F. □

Corollary 16 also gives us what one might call "the" algebraic closure of a field; any subfield of F is not an algebraic closure, as it is no longer an algebraic extension. This is what we mean above by "canonical."

A concrete example of this field F is the **algebraic numbers**, the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

5.3 4/6/22: Conjugates, Homomorphisms, and Various Examples

In this section, we will introduce the fundamental concept which will carry us until the end of the course; given $F \subset L$ a finite extension, $a \in L$, and $f(x) = \text{minpoly}(a)$, we say that any $b \in L$ so that $f(b) = 0$ is a **conjugate** of a.

In fact, vanishing on a *minimal polynomial* is a strong condition that induces the following characterization.

Lemma 28. *Suppose $F \subset L$, and $a, b \in L$. The elements a and b are conjugate if and only if they share the same minimal polynomial.*

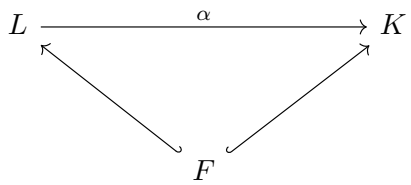
Proof. The reverse direction follows from our definition of conjugacy.

To see the forward direction, suppose that b is conjugate to a, and f is a's minimal polynomial as above. Then $\text{minpoly}(b) | f$, since $f(b) = 0$, and by f's irreducibility (Lemma 26), either $\text{minpoly}(b) = 1$ or αf for some $\alpha \in K^*$. Since $\text{minpoly}(b)(b) = 0$, the first is impossible, and since $\text{minpoly}(b)$ is monic, $\alpha = 1$. □

Corollary 17. *Conjugacy is an equivalence relation.*

The term "conjugate" is an artifact of our beloved extension $\mathbb{R} \subset \mathbb{C}$; the conjugates in the algebraic sense are in this case the conjugates in the complex sense.

As is often the case in mathematics, we will use this local property (i.e., conjugacy) to study global behavior of the spaces in which they live; to do so, we will consider the double extension $L \supset F \subset K$.



We say that a map $\alpha : L \to K$ is an F**-homomorphism** if it is a homomorphism which fixes F.

Since we often discuss extensions by only a few elements, we will generally encounter few F-homomorphisms, but the difficulty is not the size; it is determining which adjoined elements can be sent to which without violating the homomorphicity of α.

To see an example of this, consider $F = \mathbb{R}$, and $L = K = \mathbb{C}$. We claim that there are only two $\mathbb{R}$-homomorphisms $\mathbb{C} \to \mathbb{C}$. Indeed, since $i^2 = -1 \in \mathbb{R}$, such an α must satisfy $\alpha(i^2) = -1$, hence $\alpha(i) = \pm i$. Since $\mathbb{C}$ has the $\mathbb{R}$-basis $\{1, i\}$, it follows that the action of α on i totally determines the remaining values of the map; in particular, if $\alpha(i) = i$, we obtain the identity, and if $\alpha(i) = -i$, we obtain the complex conjugation map.

Significantly, we see that the minimal polynomial is invariant underneath complex conjugation; this holds for more general conjugation as well.

Theorem 52. *Suppose that L, K, F, and α are as in the formulation above. Then if $a \in L$:*

$$\text{minpoly}_F(a) = \text{minpoly}_F(\alpha(a))$$

Proof. Let $f(x) = \text{minpoly}_F(a)$. We need to show that $f(\alpha(a)) = 0$, and that f is minimal with respect to this property.

The first follows from the fact that α is an F-homomorphism:

$$f(\alpha(a)) = \sum_{i=1}^{k} c_i \alpha(a)^i = \alpha(f(a)) = 0$$

and the second trick follows from minimality: if $g(x) = \text{minpoly}_F(\alpha(a))$, then $g(x)|f(x)$, so by monicity and irreducibility $g(x) = f(x)$. □

If $L = K$, Theorem 52 takes on an equivalent formulation of conjugacy.

Corollary 18. *If $L = K \supset F$ and $\alpha : L \to K$ is an F-homomorphism, then for each $a \in L$, $\alpha(a)$ is a conjugate of a.*

For another concrete example, if $L = \mathbb{Q}[\sqrt{2}]$ and $K = \mathbb{Q}$, then the conjugates of $\sqrt{2}$ are $\sqrt{2}$ itself, and $-\sqrt{2}$. Why? Because $x^2 - 2$ is $\sqrt{2}$'s $\mathbb{Q}$-minimal polynomial.

Thus all conjugates of $\sqrt{2}$ are in $\mathbb{Q}[\sqrt{2}]$; this holds generally: quadratic extensions adjoin both conjugates, as a quadratic is only reducible into linear factors, but in this case is irreducible.

What about a higher-order problem? Let $L = \mathbb{Q}[\sqrt[3]{2}]$ and $F = \mathbb{Q}$. The rational root theorem implies that $\text{minpoly}_{\mathbb{Q}}(\sqrt[3]{2}) = x^3 - 2$, and it is not hard to see that the remaining roots of this minimal polynomial are purely complex; hence the only conjugate of $\sqrt[3]{2}$ in $\mathbb{Q}$ is itself. There is something that should be emphasized here: the conjugacy class of an algebraic element in a base field is determined just as much by the base field. It is an exercise in induction to show that every polynomial in an algebraically closed field splits into linear factors, hence the conjugacy class of any element of an algebraically closed field is just itself.

But what are the remaining roots of $x^3 - 2$? They are the third roots of unity, scaled slightly. Some easy computation gives that:

$$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$$

is a third root of unity, and $\omega^2 = \overline{\omega}$ the last. Hence the other zeroes of $x^3 - 2$ in $\mathbb{C}$ are $\sqrt[3]{2}\omega$ and $\sqrt[3]{2}\omega^2$. To find their minimal polynomial in $\mathbb{Q}[\sqrt[3]{2}]$, compute $(x^3 - 2)/(x - \sqrt[3]{2})$.

We have now found that the conjugacy class of $\sqrt[3]{2}$ in $\mathbb{Q} \subset \mathbb{C}$ is $\{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\}$, but now we have an intermediary field $\mathbb{Q}[\sqrt[3]{2}]$, with $\mathbb{Q}$-basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. What is the $(\mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{C})$-conjugacy class of an arbitrary element

$$a + b\sqrt[3]{2} + c\sqrt[3]{4}$$

in this new field?

This seems kind of rough to compute explicitly. Instead, we will do something better. Addition in this basis is done coordinatewise, so to understand $\mathbb{Q}[\sqrt[3]{2}]$, we need only understand the multiplication table of its elements. If $x = \sqrt[3]{2}$, it is:

$\cdot$	1	x	x^2
1	1	x	x^2
x	x	x^2	2
x^2	x^2	2	$2x$

On the other hand, if $y = \sqrt[3]{2}\omega$ (it's not hard to see that adjoining y will give a degree 3 extension), we have the multiplication table:

$\cdot$	1	y	y^2
1	1	x	y^2
y	y	y^2	2
y^2	y^2	2	$2y$

We have explicitly demonstrated that the map $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$ from $\mathbb{Q}[\sqrt[3]{2}]$ to $\mathbb{Q}[\sqrt[3]{2}\omega]$ is a $\mathbb{Q}$-homomorphism.

Since $\mathbb{Q}$-homomorphic elements have the same minimal polymomial, it follows that the conjugacy class of $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ is

$$\{a + b\sqrt[3]{2} + c\sqrt[3]{4}, a + b\sqrt[3]{2}\omega + c\sqrt[3]{4}\omega^2, a + b\sqrt[3]{2}\omega^2 + c\sqrt[3]{4}\omega\}$$

And this is the entire conjugacy class, as the total extension is degree 6, and we are working in an intermediary field of degree 2 over $\mathbb{Q}$, hence the minimal polynomial of $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ in $\mathbb{Q}[\sqrt[3]{2}, x]$ is degree at most 3.

5.4 4/8/22: Splitting Fields and Multiple Roots

We start this section with a coda on the last, which foreshadows where the theory is heading. Let $K = \mathbb{Q}[\sqrt[3]{2}, \omega]$; i.e., the degree six extension of $\mathbb{Q}$ given by the roots of $x^3 - 2$. We claim that there are 6 $\mathbb{Q}$-automorphisms of K. Indeed, we let α fix $\mathbb{Q}$, and observe that if we wish to extend α to K, we need to pick where it sends $\sqrt[3]{2}$ and ω. The supposed six possibilities are given by the independent choices:

$$\alpha(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\} \text{ and } \alpha(\omega) \in \{\omega, \omega^2\}$$

And some direct computation shows that all six options are indeed $\mathbb{Q}$-homomorphisms.

The example we've been working with is an example of a more general construction, which we will discuss in this section. Suppose $f \in F[x]$. We say that L is a **splitting field of** $f(x)$, alternatively called a **root field**, if:

1. $f(x) = c\prod_{i=1}^{n}(x - \alpha_i)$, where each $\alpha_i \in L$; i.e., f **splits** in L
2. $L = K[\alpha_1, \ldots, \alpha_n]$.

Hence K is a splitting field of $x^2 - 2 \in \mathbb{Q}[x]$. We will now show that such a splitting field holds for any polynomial.

Theorem 53. *Suppose $f(x) \in F[x]$. Then there exists a splitting field for f.*

Proof. This is a straightforward induction on the degree of f. If f is degree 1, we are done.

If f has degree $n \geqslant 2$, then take any irreducible factor f_1 of f in $F[x]$ of degree at least 2 (we can assume f has no linear factors in $F[x]$). If every conjugate of f is in $F[x]/\langle f_1\rangle$, we can take $F[x]/\langle f_1\rangle$ to be f's splitting field. Otherwise, f/f_1 is in $F[x]/\langle f_1\rangle$, and is of strictly lower degree, so by induction we can find a splitting field of f/f_1, which is a splitting field of f. □

Uniqueness will require a little more grit.

Theorem 54. *Let $f(x) \in F[x]$, and $E = F[\alpha_1, \ldots, \alpha_k]$ so that for every i, $f(\alpha_i) = 0$. If Ω is a splitting field of f, then:*

1. *There is an F-homomorphism $\pi : E \to \Omega$, and*
2. *The different π number at most $[E : F]$.*

Proof. Write $F_i = F[\alpha_1, \ldots, \alpha_i]$; hence $F_k = E$. We may assume $F \neq F_1$; then α_1 is a root of some irreducible factor of $f(x)$ of degree at least 2. Define $\pi_1 : F_1 \to \Omega$ by sending α_1 to any root of this factor. This evidently fixes F. Proceed in this fashion, sending each α_j to a zero of $\text{minpoly}_{F_{j-1}}(\alpha_j)$. Hence we get a full extension $E \to \Omega$ which fixes F, and by construction, these extension number:

$$[E : F_{k-1}] \ldots [F_2 : F_1][F_1 : F] = [E : F]$$

□

It is worth noting that the bound is not an equality because an irreducible polynomial may have fewer distinct roots than its degree.

This is enough to give uniqueness:

Corollary 19. *A splitting field is unique up to isomorphism.*

Proof. Consider two splitting fields Ω, Ω' of f. By Theorem 54, there are $\pi : \Omega' \to \Omega$ and $\pi' : \Omega \to \Omega'$ which fix F, hence we can compose to obtain an F-homomorphism $\pi \circ \pi' : \Omega \to \Omega$. This is a linear map of a finite-dimensional vector space, hence is injective if and only if it is surjective. All field homomorphisms are injective, so it is surjective, thus π is surjective (if $\pi \circ \pi'$ has right inverse g, then π has right inverse $(\pi' \circ g)$), hence an isomorphism. □

Slick.

As mentioned above, things can go wrong when polynomials have multiple roots. Thankfully, there's an easy way to check this.

Theorem 55. *A polynomial $f(x) \in F[x]$ has distinct roots in some extension $K \supseteq E$ if and only if:*

$$\gcd\left(f(x), \frac{d}{dx}f(x)\right) \neq 1$$

Proof. Let α_i be the roots of f in f's splitting field. Then $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$ and $f'(x) = \sum_{i=1}^{n}\prod_{j\neq i}(x - \alpha_j)$.

From this, we can see that $\gcd(f, f') \neq 1 \Leftrightarrow \alpha_i = \alpha_j$ for $i \neq j$.

□

In fact, we can say something more general.

Theorem 56. *Suppose char$(F) = 0$. If $f(x) \in F[x]$ is irreducible, it has no multiple zeroes in any extension of F.*

In particular, a polynomial irreducible over $\mathbb{Q}$ cannot have multiple zeroes in $\mathbb{C}$.

Proof. This follows from the previous theorem. Since f is irreducible, it holds that $f' \not| f$. To show $\gcd(f, f') = 1$, it suffices to show that $f \not| f'$. Indeed, if $f(x) = \sum a_i x^i$, then $f'(x) = \sum i a_i x^{i-1}$. Since F is characteristic 0, $f' \neq 0$, and we are done— f is higher degree than f', so it cannot divide it. □

This can fail (very badly) in characteristic p. Indeed, let F have characteristic p, and suppose $a \in F$ is so that $a \neq b^p$ for every $b \in F$. Then $x^p - a$ is irreducible, but in its splitting field it has only one root of multiplicity p. In Ω it holds that $a = b^p$, so $x^p - a = x^p - b^p = (x - b)^p$.

The proof fails because $f'(x) = px^{p-1} = 0$ in characteristic p, hence $\gcd(f, f') = f$.

5.5 4/11/22: Perfect Fields

This section discusses a measurement of how "bad" a field can be with respect to multiple roots, elaborating upon the example at the end of last section.

We say a field F is **perfect** if $\text{char}(F) = 0$, or $\text{char}(F) = p$ and every element of F has a pth root. Here are three examples:

1. If F is algebraically closed, it must be perfect: $x^p - a$ has a root in F.
2. $\mathbb{Z}/p\mathbb{Z}$ is perfect, by Fermat's Little Theorem ($a^p \equiv_p a$)
3. Every finite field is perfect; consider the **Frobenius map** $\varphi : x \mapsto x^p$. Since F is characteristic p, φ is an automorphism:

$$(x_1 + x_2)^p = \sum_{k=0}^{p} \binom{p}{k} x_1^k x_2^{p-k} = x_1^p + x_2^p$$

   By field theory, this implies that φ is injective, hence by $|F| < \infty$ it is also surjective, and thus F is perfect.

A nonexample is $\mathbb{Z}/p\mathbb{Z}(x)$; by the existence of a reduced form representation, x has no pth root.

Why do we care about perfect fields? We say a polynomial is **separable** if it has distinct roots in every extension; thus Theorem 56 may be rephrased: "if $f(x) \in F[x]$ is irreducible, it is separable." Perfection is a global guarantee of the local property of separability:

Lemma 29. *Suppose F is perfect and $f(x)$ is irreducible. Then f is separable.*

Proof. The case $\text{char}(F) = 0$ is covered by Theorem 56. Suppose $\text{char}(F) = p$ and further suppose for the sake of contradiction that $f(x) = g(x^p)$; i.e., that f has multiple roots. We write $g(x) = \sum_{i=0}^{j} a_i x^i$, and by perfection, each a_i is b_i^p for some $b_i \in F$, so:

$$f(x) = g(x^p) = \sum_{i=0}^{k} b_i^p x^{pi} = \left(\sum_{i=0}^{k} b_i x^i \right)^p = g(x)^p$$

which contradicts irreducibility. □

We also get a nice partial converse:

Lemma 30. *Suppose* $\text{char}(F) = p$ *and F is not perfect; if there exists $a \in F$ so that $x^p - a$ has no roots in F, then:*

1. *$x^p - a$ is irreducible in $F[x]$, and*
2. *$x^p - a$ has multiple roots in some extension.*

Proof. To see (2), let $\Omega \supset F$ be F's splitting field with respect to $x^p - a$; then there is $b \in \Omega$ so that $b^p = a$. Then $x^p - a = x^p - b^p = (x-b)^p$.

To prove (1), suppose $x^p - a$ is $g(x)h(x)$ in $F[x]$, where h and g are monic. In $\Omega[x]$, the only monic factors of $(x-b)^p$ are $(x-b)^k$ for $0 \leqslant k \leqslant p$. Hence $g(x) = (x-b)^k$ and $h(x) = (x-b)^{p-k}$, for some k.

Suppose for contradiction that $k \in \{1, \ldots, p-1\}$. By Bezout's Lemma, there is some $n \in \mathbb{Z}$ so that $kn \equiv 1 \pmod{p}$, hence as $g(x)^n$ is in $F[x]$, this is just $(x-b) \in F[x]$, contradicting that $b \notin F$. □

We conclude the section by discussing the more general theory of finite fields, as finite fields are always perfect and will be a fruitful source of examples.

Theorem 57. *Suppose F is a finite field of characteristic p. Then $|F| = p^n$ for some n.*

Proof. Since $\mathrm{char}(F) = p$, it follows that $\langle 1 \rangle \cong \mathbb{Z}/p\mathbb{Z}$ is a subfield, hence F is a vector space over $\langle 1 \rangle$; the theorem follows from the uniqueness of basis representation of vector spaces. □

Theorem 58. *For every p prime, and $n \in \mathbb{N}$, every field F is $|F| = p^n$ is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}/p\mathbb{Z}$. Moreover, $x^{p^n} - x = \prod_{\alpha \in F}(x - \alpha)$.*

The second result merits a note: in general, the roots of a polynomial generate its splitting field, but in this case they *form* the splitting field.

Proof. Recall the multiplicative group of a finite field is cyclic, of order $p^n - 1$. By Lagrange's Theorem, for every $x \neq 0$ in F, $x^{p^n - 1} = 1$, so for every $x \in F$ it follows that $x^{p^n} - x = 0$. By the degree bound for roots of a polynomial, it follows that $x^{p^n} - x$ splits in F, and by counting is $\prod_{\alpha \in F}(x - \alpha)$. □

Corollary 20. *For every $n \in \mathbb{N}$ and p prime, there is a field F so that $|F| = p^n$*

Proof. Take the splitting field Ω of $x^{p^n} - x$ over $\mathbb{Z}/p\mathbb{Z}$. The zeroes of this polynomial form a subfield of Ω (this uses the Frobenius automorphism), and by minimality of the splitting field, it follows that Ω is the F we seek. □

Corollary 21. *There is exactly one degree n extension of $\mathbb{Z}/p\mathbb{Z}$, up to isomorphism.*

This follows from uniqueness of the splitting field.

Theorem 59. *Suppose $|F| = p^n$. Then the subfields of F are the following; for each $k|n$:*

$$F_k = \{x \in F : x^{p^k} - x = 0\}$$

Proof. Simply observe that F_k is a field, and conclude by Corollary 21 that all subfields of F are of this form. □

5.6 4/13/22: Reinterpreting Field Extensions: Counting F-Homomorphisms

Suppose $E \supset F$ is a field extension. Then:

$$\mathrm{Aut}(E/F) = \{\alpha \in E^E : \alpha \text{ is a surjective } F\text{-homomorphism}\}$$

is a group with respect to composition.

The following lemma says we can omit surjectivity if $E \supset F$ is finite.

Lemma 31. *If $F \subset E$ is finite, then every F-homomorphism $\alpha : E \to E$ is invertible.*

Proof. By Theorem 52, $[\alpha(E) : F] = [E : F]$, and since $F \subseteq \alpha(E) \subseteq E$, it follows that $[E : F] = [E : \alpha(E)][\alpha(E) : F]$, hence $[E : \alpha(E)] = 1$, so $f(E) = E$ and f is surjective. Injectivity follows from field theory.

□

Next, we will consider a tower $E \supset F \subset E'$. As is expected, finiteness of the domain extension has bearing in the number of F-homomorphisms from E to E'.

Theorem 60. *Suppose $F \subset E$ is a finite extension, and $F \subset E'$ is an extension. Then the number of F-homomorphisms $\alpha : E \to E'$ is at most $[E : F]$.*

Proof. We write $E = F[a_1, \ldots, a_n]$, and perform induction on n.

If $E = F[a]$ for some $a \in E$, then writing $f = \mathrm{minpoly}_F(a)$, since any polynomial has at most its degree's worth of roots in any field, it follows that $f(x)$ has at most $[E : F]$ roots in E'.

Since each F-homomorphism $\alpha : E \to E'$ sends a to another root of f, each such α is totally determined by our choice of a root of f in E', proving the base case.

The inductive step follows from the multiplicativity of the degree, and basic counting.

□

Corollary 22. *Suppose $f \in F[x]$, and $E = F[x]/\langle f \rangle$. Then $|\mathrm{Aut}(E/F)| \leqslant [E : F]$.*

For example, $\mathrm{Aut}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}) = \{e\}$. To riff off of the previous sections, if $\mathrm{char}(F) = p$ and $a \in F$ has no pth root, and $E = F[x]/\langle x^p - a \rangle$, then $\mathrm{Aut}(E/F) = \{e\}$. After all, by the previous sections, E is essentially $F[b]$, and there is only one F-automorphism of $F[b]$.

When the the bound in Theorem 60 sharp? Here is a sufficient condition (which we have seen in action!)

Theorem 61. *Suppose $F \subset E$ is finite and E is F-generated by $\{a_1, \ldots, a_n\}$, each a_i with minimal polynomial f_i. If each f_i is separable and $\prod f_i$ splits in E', then the number of F-homomorphisms $E \to E'$ is precisely $[E : F]$.*

Proof. The reasoning is essentially similar to Theorem 60. The base case is easy to see. We write $F_i = F_{i-1}[a_i]$, where $F = F_0$.

Suppose $g_i = \mathrm{minpoly}_{F_{i-1}}(a_i)$. Observe $g_i | f_i$ in $F_{i-1}[x]$. so g_i is separable by hypothesis. Since $\prod f_i$ splits in E', then $\alpha(g_i)$ splits in $E'[x]$ as a product of $\deg(g_i)$ factors.

Hence we have $\deg(g_i)$ choices at each step of the induction by which we extend α from F_{i-1} to F_i. Multiplicativity of the degree finishes the proof. $\square$

Corollary 23. *Suppose $f \in F[x]$ is separable, and E a splitting field of f. Then $|\mathrm{Aut}(E/F)| = [E : F]$.*

To avoid the problematic cases following Corollary 22, we say an algebraic extension $F \subset E$ is **normal** if for any $a \in E$, it holds that $\mathrm{minpoly}_F(a)$ splits in E, and is **separable** if for every $a \in E$, $\mathrm{minpoly}_F(a)$ is separable. In general, an algebraic extension of a perfect field is perfect and separable.

This is where we are heading: we say an extension $F \subset E$ is **Galois** if and only if it is both normal and separable. If $F \subset E$ is a Galois extension, we write $\mathrm{Gal}(E/F) = \mathrm{Aut}(E/F)$, the **Galois group of** $E \subset F$. Galois extensions are the right things to think about, as it turns out.

5.7 4/19/22: What is a Galois Extension?

Recall that if an extension $F \subset E$ is both normal and separable, the extension is **Galois**.

Suppose $F \subset E$ is an extension, and G is a group of automorphisms of E. In this case, we write $E^G = \{a \in E : g(a) = a, \forall g \in G\}$.

Theorem 62. *Let $F \subset E$ be an extension, and G a group of automorphisms of E. Then $[E : E^G] \leqslant |G|$.*

Proof. Let $G = \{\sigma_1, \ldots, \sigma_m\}$, where $\sigma_1 = e$. We will show that any set $\{\alpha_1, \ldots, \alpha_n\} \subseteq E$ with $n > m$ is linearly independent over E^G. Indeed, consider $\Sigma\mathbf{x} = \mathbf{0}$, where $\Sigma_{ij} = \sigma_i(\alpha_j)$. Since Σ is an $m \times n$ matrix where $n > m$, it follows that the corresponding homogenous system has a nontrivial solution in E. Pick $\mathbf{c} \in \text{null}(\Sigma)$ with the smallest support; up to permutations and scaling, we may assume that $0 \neq c_1 \in E^G$.

Suppose for contradiction that some c_j is not in E^G; then $\sigma_k(c_j) \neq c_j$ for some $k \neq 1$ and $j \neq 1$. Since each σ_k is a homomorphism, and each σ_k permutes G, it follows that $\sigma_k(\Sigma\mathbf{c}) = \sigma_k(\mathbf{0})$ is nothing but $\Sigma\sigma_k(\mathbf{c}) = \mathbf{0}$, hence $(\tilde{\mathbf{c}})_i = \sigma_k(c_i) \in (\Sigma)$. Since $\sigma_k(c_i) - c_i \neq 0$, it follows that $\tilde{\mathbf{c}} - \mathbf{c} \neq \mathbf{0}$, but since $(\tilde{\mathbf{c}})_1 = c_1$, we have a contradiction: $\text{supp}(\tilde{\mathbf{c}} - \mathbf{c}) < \text{supp}(\mathbf{c})$.

Hence $\mathbf{c} \in (E^G)^n \cap \text{null}(\Sigma)$, so the first row gives $\sum_{i=1}^n \sigma_1(\alpha_i)c_i = 0$, which is nothing but the E^G-linear combination $\sum a_i c_i = 0$ where $c_1 \neq 0$, giving that $\{\alpha_1, \ldots, \alpha_n\}$ is linearly dependent over E^G.

□

Corollary 24. *Let $E \supset F$ be a finite extension, and G a group of automorphisms of E. Then $G = \text{Aut}(E/E^G)$.*

Proof. By Theorem 60, $|\text{Aut}(E/E^G)| \leqslant [E : E^G]$. Next, observe that every $g \in G$ is a surjective E^G-homomorphism of E, so $g \in \text{Aut}(E/E^G)$. It follows by Theorem 62 that $[E : E^G] \leqslant |G| \leqslant |\text{Aut}(E/E^G)|$, thus as $G \subseteq \text{Aut}(E/E^G)$ and $|G| = |\text{Aut}(E/E^G)|$, the result follows by finiteness. □

Theorem 63 (Classification of Galois Extensions)**.** *For an extension $E \supset F$, the following are equivalent:*

1. *E is the splitting field of some separable $f \in F[x]$,*
2. *$[E : F] < \infty$ and $F = E^{\text{Aut}(E/F)}$,*
3. *$F = E^G$ for some finite $G \subseteq \text{Aut}(E/F)$,*
4. *$E \supset F$ is finite Galois.*

Proof. We will show each implies the next, mod 4.

(1) ⇒ (2): Suppose E is the splitting field of a separable $f \in F[x]$. We get $[E : F] < \infty$ by Theorem 49. Let $G = \text{Aut}(E/F)$. By Corollary 23, $|G| = [E : F]$. By the work done in Corollary 24, it also holds that $|G| = [E : E^G]$, and since $F \subseteq E^G \subseteq E$, it follows by multiplicativity of the degree that $[E^G : F] = 1$, hence $E^{\text{Aut}(E/F)} = F$.

(2) $\Rightarrow$ (3): Since $[E : F] < \infty$, it follows that $\mathrm{Aut}(E/F)$ is finite, so let $G = \mathrm{Aut}(E/F)$.

(3) $\Rightarrow$ (4): Suppose $F = E^G$ for some finite $G \subseteq \mathrm{Aut}(E/F)$. Then $[E : F] = [E : E^G] \leqslant |G|$, by Theorem 62, hence the extension $E \supset F$ is finite. We with to show that for each $a \in E$, $\mathrm{minpoly}_{E^G}(a)$ splits into distinct factors in $E[x]$.

Let $\alpha \in E$, and $f = \mathrm{minpoly}_{E^G}(\alpha)$. Let $\{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m\} = G \cdot \{\alpha\}$, and let $g(x) = \prod_{i=1}^{m}(x - \alpha_i)$. Since the coefficients of g are symmetric in the α_i, and $\sigma \in G$ permutes the α_i, it follows that $g(x) \in E^G[x]$. Since $g(\alpha) = 0$ and g is monic, it follows that $f|g$, and since $f \in E^G[x]$:

$$f(\alpha) = 0 \Longrightarrow \sigma(f(\alpha)) = 0 \Longrightarrow f(\alpha_i) = 0$$

Hence each root fo g is a root of f, thus $g|f$. By monicity, $g = f$, so $f(x)$ splits into distinct factors in E. The extension is Galois.

(4) $\Rightarrow$ (1): Since $[E : F] < \infty$, it follows from Theorem 46 that $E = F[\alpha_1, \ldots, \alpha_m]$, where each $\alpha_i \in E$ and is algebraic over F.

Let $f_i = \mathrm{minpoly}_F(\alpha_i)$, and $f = \prod_{i=1}^{m} f_i$. By normality, E is the splitting field of f, and by separability, f is separable.

□

It is then reasonable to call a field extension satisfying any one of the conditions of Theorem 63 a finite Galois extension. In any of these cases, we write $\mathrm{Gal}(E/F) = \mathrm{Aut}(E/F)$.

Corollary 25. *Suppose $F \subset M \subset E$, and $E \supset F$ is finite Galois. Then $E \supset M$ is finite Galois.*

Proof. This is two applications of Theorem 62. Since $E \supset F$ is finite Galois, it follows that E is the splitting field of some f separable in $F[x]$. f is also in $M[x]$, and is still separable, hence $E \supset M$ is finite Galois. □

It is worth verifying that $\mathbb{Q}[\sqrt[3]{2}, \omega] \supset \mathbb{Q}$, the example we have worked with before, satisfies each of these conditions.

5.8 4/20/22: The Fundamental Theorem of Galois Theory

This section is dedicated to the most significant theorem in Galois Theory. Let $E \supseteq F$ be a finite Galois extension, where $G = \mathrm{Gal}(E/F)$. The theorem amounts to stating that there is an extremely well-behaved one-to-one correspondence between intermediate extensions $F \subseteq M \subseteq E$, and subgroups $\{e\} \leq H \leq G$, given by the two maps:

$$f : \begin{cases} \{\text{intermediate extensions}\} \to \{\text{subgroups}\} \\ M \mapsto \mathrm{Gal}(E/M) \end{cases}$$

$$g : \begin{cases} \{\text{subgroups}\} \to \{\text{intermediate extensions}\} \\ H \mapsto E^H \end{cases}$$

Theorem 64 (Fundamental Theorem of Galois Theory)**.** *The maps f and g described above are inverses, and if $H_1, H_2 \leq G$, the correspondence they describe:*

1. *Is inclusion-reversing: $H_1 \subseteq H_2 \iff E^{H_1} \subset E^{H_2}$.*
2. *Indexes degrees: $[H_1 : H_2] = [E^{H_2} : E^{H_1}]$.*
3. *Maps conjugates to automorphic images: $\sigma H \sigma^{-1} \longleftrightarrow \sigma M$.*
4. *Preserves normality: $H \triangleleft G \iff E^H \supset F$ is normal. Moreover, if $H_1 \triangleleft G$, then $\mathrm{Gal}(E^H/F) \cong G/H$.*

Proof. First we prove that these maps are inverses. Let $H \leq G$. Then $F \subset E^H \subset E$, and by Corollary 25, $E^H \subset E$ is finite Galois, hence by Corollary 24, $H = \mathrm{Gal}(E/E^H)$, so $f \circ g = \mathrm{id}$. Now suppose $F \subset M \subset E$. Again by Corollary 25, $M \subset E$ is finite Galois, so by Theorem 63, $E^{\mathrm{Gal}(E/M)} = M$, so $g \circ f = \mathrm{id}$. Both maps are defined on their domains, hence are inverse bijections.

Now we show the remaining properties.

1. We will show (1) by each direction. Suppose $M_1 \subseteq M_2$ are intermediate extensions. This relation implies that $\mathrm{Gal}(E/M_2) \subseteq \mathrm{Gal}(E/M_1)$.

   Now suppose that $H_2 \subseteq H_1$. This implies that $E^{H_1} \subseteq E^{H_2}$, completing this part of the proof.

2. Suppose we have the following correspondences:

$$F \subseteq M_1 \subseteq M_2 \subseteq E$$

$$G \geq H_1 \geq H_2 \geq \{e\}$$

   By finite Galois, $[E : M_i] = |H_i|$ for each i, hence:

$$[M_2 : M_1] = \frac{[E : M_1]}{[E : M_2]} = \frac{|H_1|}{|H_2|} = [H_1 : H_2]$$

3. Consider another correspondence-pair $F \subseteq M \subseteq E$ and $G \geq H \geq \{e\}$, and let $\sigma \in G$. Then:

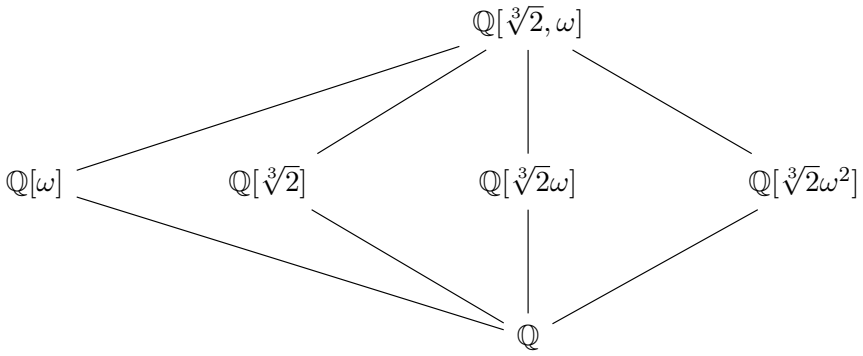
$$\begin{aligned}
\gamma \in \mathrm{Gal}(E/\sigma M) &\Leftrightarrow \gamma \in G \text{ s.t. } \forall x \in \sigma M, \gamma(x) = x \\
&\Leftrightarrow \forall y \in M, \gamma(\sigma(y)) = \sigma(y) \\
&\Leftrightarrow \forall y \in M, \sigma^{-1}\gamma\sigma(y) = y \\
&\Leftrightarrow \sigma^{-1}\gamma\sigma \in H \\
&\Leftrightarrow \gamma \in \sigma H \sigma^{-1}
\end{aligned}$$

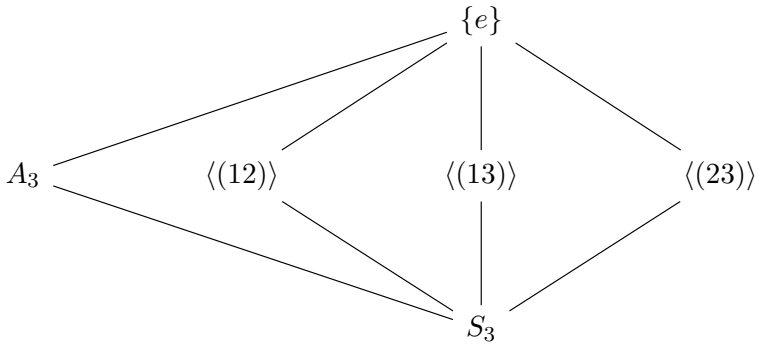
4. Recall that the conjugates of elements of M are nothing but $\sigma(a)$ for various $\sigma \in G$. By part 3, the condition $\forall \sigma \in G$, $\sigma(a) \in M$ is equivalent to the condition that $\forall \sigma \in G$, $\sigma H \sigma^{-1} = H$. However, this is nothing but the statement that $F \subset M$ is normal if and only if $\mathrm{Gal}(M/F) \triangleleft G$.

   To see the second claim, we construct a surjection $\pi : G \to \mathrm{Gal}(E^H/F)$ whose kernel is H. Indeed, simply take the restriction of each element of G to M; let $\pi(\sigma) = \sigma|_M \in \mathrm{Gal}(M/F) = \mathrm{Gal}(E^H/F)$. In this case, $\ker(\pi) = \{\sigma \in G : \sigma|_M = \mathrm{id}\} = H$, and surjectivity follows from degree counting. The first isomorphism theorem gives the result.

□

The example we have worked with gives some good intuition; on the next page are Hasse diagrams of the correspondence of subfields of $\mathbb{Q}[\sqrt[3]{2}, \omega]$, and subgroups of S_3.


$\mathbb{Q}[\sqrt[3]{2},\omega]$
$\mathbb{Q}[\omega]$
$\mathbb{Q}[\sqrt[3]{2}]$
$\mathbb{Q}[\sqrt[3]{2}\omega]$
$\mathbb{Q}[\sqrt[3]{2}\omega^2]$
$\mathbb{Q}$


$\{e\}$
A_3
$\langle(12)\rangle$
$\langle(13)\rangle$
$\langle(23)\rangle$
S_3

5.9 4/22/22: Transcendence Bases

Congrats, you made it to the last section!

We have done a lot of thinking about fields as vector spaces over subfields, and with that notion comes a basis. However, that only captures *linear* dependence between extending elements; another (coarse) metric for size of fields over subfields may be a kind of *algebraic* dependence, where a polynomial relation is what must be satisfied.

Suppose $F \subset \Omega$ is the splitting field of F. We say that $\{a_1, \ldots, a_n\} \subset \Omega$ are **algebraically dependent** over F if there is a nonzero polynomial $p \in F[x_1, \ldots, x_n]$ such that $p(a_1, \ldots, a_n) = 0$. Otherwise, we say that the $\{a_1, \ldots, a_n\}$ are **algebraically independent**.

Despite being motivated by linear algebra, this cutely generalizes our previous work: $\{a_1\}$ is algebraically dependent over F if and only if a_1 is algebraic over F.

Here is an example: let $F = \mathbb{Q}$, and $\Omega = \mathbb{C}$. Let $a_1 = \pi^2$ and $a_2 = \sqrt{\pi^3 - 1}$. Observe that $p(x_1, x_2) = x_1^3 - (x_2^2+1)^2$ satisfies $p(a_1, a_2) = 0$, hence $\{\pi^2, \sqrt{\pi^3 - 1}\}$ is algebraically dependent over $\mathbb{Q}$.

We can generalize further. Suppose $A \subset \Omega$; we say that A is **algebraically independent** over F if any finite subset of A is algebraically independent over F.

More general yet, if $B \subset \Omega$, we say that A is **algebraically dependent on** B if for each $a \in A$, there is a finite subset $B' \subset B$ so that a is algebraic over $F(B')$.

[I believe this is equivalent to the statement that any finite subset of A is algebraically dependent over $F(B')$, for some $B' \subset F$ finite.]

The next theorem gives an equivalent formulation which furthers the parallels with linear dependence.

In fact, for flavor the algebraically independent sets form the independent sets of a matroid!

Theorem 65. *$\{a_1, \ldots, a_n\}$ are algebraically dependent if and only if there is some i so that a_i is algebraically dependent on $\{a_1, \ldots, \widehat{a_i}, \ldots, a_n\}$.*

Proof. Suppose $\{a_1, \ldots, a_n\}$ are algebraically dependent. Then there is some $0 \neq p \in F[x_1, \ldots, x_n]$ so that $p(a_1, \ldots, a_n) = 0$.

If x_i is not involved in p's definition, we are done. So we may say:

$$p(\mathbf{x}) = \sum_{k=0}^{N} x_i^k q_k(x_1, \ldots, \widehat{x_i}, \ldots, x_n)$$

Since $p(\mathbf{a}) = 0$, this formulation of p shows that we may consider $p \in F[a_1, \ldots, \widehat{a_i}, \ldots, a_n, x]$ so that $p(a) = 0$, which is precisely what we wished to show.

Now suppose that a_i is algebraic over $F(a_1, \ldots, \widehat{a_i}, \ldots, a_n)$. Then there exists a polynomial:

$$\sum_{k=0}^{N} x^k p_k(a_1, \ldots, \widehat{a_i}, \ldots, a_n)$$

which vanishes at a_i. Substituting x_j for a_j gives what we sought. □

We say that $A \subset \Omega$ is a **transcendence basis** of Ω over F if:

1. A is algebraically independent over F, and
2. every $b \in F$ is algebraic over A.

Next, we shall prove a theorem which parallels the fact that an independent set in the span of another set has bounded cardinality.

Theorem 66. *Suppose $A = \{a_1, \ldots, a_m\}$ and $B = \{b_1, \ldots, b_n\}$ so that:*

1. *A is algebraically independent over F, and*
2. *A is algebraically dependent on B.*

Then $m \leqslant n$.

To prove this, we will use two lemmas.

Lemma 32 (Algebraic Exchange Property)**.** *If β is algebraically dependent on $\{\alpha_1, \ldots, \alpha_m\}$ but not on $\{\alpha_1, \ldots, \alpha_{m-1}\}$, then α_m is algebraically dependent on $\{\alpha_1, \ldots, \alpha_{m-1}, \beta\}$.*

Proof. Since β is algebraically dependent on $\{\alpha_1, \ldots, \alpha_m\}$, there is a polynomial in $F[\alpha_1, \ldots, \alpha_m, x]$:

$$p(x) = \sum_{i=1}^{N} q_i(\alpha_1, \ldots, \alpha_m) x^i$$

so that $p(\beta) = 0$. Substituting α_i with y_i, we can write:

$$p(y_1, \ldots, y_m, x) = \sum_{i=1}^{k} y_m^k r_i(y_1, \ldots, y_{m-1}, x)$$

and observe that if each of the r_i were 0, then p would be 0. Moreover, as β is algebraically independent of $\{\alpha_1, \ldots, \alpha_{m-1}\}$, it follows that that nonzero polynomial is nonzero on $\{\alpha_1, \ldots, \alpha_{m-1}, \beta\}$. Hence p in fact certifies that α_m is algebraically dependent on $\{\alpha_1, \ldots, \alpha_{m-1}, \beta\}$. □

Lemma 33. *Algebraic dependence is transitive.*

Now we can prove the theorem.

Proof of Theorem 66. We may write $B = \{a_1, \ldots, a_k, b_{k+1}, \ldots, b_k\}$. If $k = m$, then $A = B$, so certainly $m = n$.

Suppose $k < m$. Since a_{k+1} is algebraically dependent on $\{a_1, \ldots, a_k, b_{k+1}, \ldots, b_n\}$ but not on $\{a_1, \ldots, a_k\}$, it follows that there is some b_j, where $k + 1 \leqslant j \leqslant n$, so that a_{k+1} is algebraically independent of $\{a_1, \ldots, a_k, b_{k+1}, \ldots, a_{j-1}\}$ but dependent on $\{a_1, \ldots, a_k, b_{k+1}, \ldots, a_j\}$. By the algebraic exchange property, b_j is algebraically dependent on $B' = B \cup \{a_{k+1}\} \setminus \{b_j\}$.

Thus B is dependent on B', hence by transitivity A is dependent on B'. We repeatedly exchange, and eventual termination gives the result.

□

We get directly:

Corollary 26. *Suppose A and B are two finite transcendence bases of Ω. Then $|A_1| = |A_2|$.*

We write the number $|A_1|$ of Corollary 26 as $\operatorname{trdeg}(\Omega/F)$. If F is a finite extension of E, then $\operatorname{trdeg}(F/E) < \infty$.

Theorem 67. *Suppose $F \subset E \subset L$. Then:*

$$\operatorname{trdeg}(L/F) = \operatorname{trdeg}(L/E) + \operatorname{trdeg}(E/F)$$

Proof. Suppose $A = \{a_1, \ldots, a_n\}$ is a transcendence basis of E/F, and $B = \{b_1, \ldots, b_m\}$ is a transcendence basis of L/F. It suffices to show that $A \cup B$ is a transcendence basis of L/F.

Suppose for contradiction that there is a polynomial $p \neq 0$ in $F[x_1, \ldots, x_n, y_1, \ldots, y_m]$ which vanishes at $A \cup B$ (assigning indices appropriately). We can view p as a polynomial in the y_i, with coefficients polynomials in the x_j with coefficients in F. Since A is independent over F, it follows that assigning $x_j = a_j$ produces a polynomial in $F[a_1, \ldots, a_n, y_1, \ldots, y_m]$ which is nonzero, but vanishes on B. This is a polynomial in $E[y_1, \ldots, y_m]$ which is nonzero but vanishes on B, contradicting that B is independent over E.

Therefore $A \cup B$ is independent over F.

To show that every $a \in L$ is algebraically dependent on $A \cup B$, we use the classic trick: every $a \in L$ is the root of a polynomial in $E[b_1, \ldots, b_m]$, whose coefficients are algebraic over $F[a_1, \ldots, a_n]$, thus by multiplicativity of the degree, the extension $F \subset F[a_1, \ldots, a_n, b_1, \ldots, b_m]$ is finite, hence algebraic, hence the extension $F[A \cup B] \subset F[A \cup B, c]$ is finite, hence algebraic. □