Algebra

D. Zack Garza

January 7, 2020

Contents

1 Thursday August 15th

We'll be using Hungerford's Algebra text.

1.1 Definitions

The following definitions will be useful to know by heart:

- The order of a group
- Cartesian product
- Relations
- Equivalence relation
- Partition
- Binary operation
- Group
- Isomorphism
- Abelian group
- Cyclic group
- Subgroup
- Greatest common divisor
- Least common multiple
- Permutation
- Transposition

- Orbit
- Cycle
- The symmetric group S_n
- The alternating group A_n
- Even and odd permutations
- Cosets
- Index
- The direct product of groups
- Homomorphism
- Image of a function
- Inverse image of a function
- Kernel
- Normal subgroup
- Factor group
- Simple group

Here is a rough outline of the course:

- Group Theory
  - Groups acting on sets
  - Sylow theorems and applications
  - Classification
  - Free and free abelian groups
  - Solvable and simple groups
  - Normal series
- Galois Theory
  - Field extensions
  - Splitting fields
  - Separability
  - Finite fields
  - Cyclotomic extensions
  - Galois groups
  - Solvability by radicals
- Module theory
  - Free modules
  - Homomorphisms
  - Projective and injective modules
  - Finitely generated modules over a PID
- Linear Algebra
  - Matrices and linear transformations
  - Rank and determinants
  - Canonical forms
  - Characteristic polynomials
  - Eigenvalues and eigenvectors

1.2 Preliminaries

Definition: A **group** is an ordered pair $(G, \cdot : G \times G \to G)$ where G is a set and $\cdot$ is a binary operation, which satisfies the following axioms:

1. **Associativity**: $(g_1 g_2) g_3 = g_1 (g_2 g_3)$,
2. **Identity**: $\exists e \in G \;\middle|\; ge = eg = g$,
3. **Inverses**: $g \in G \implies \exists h \in G \;\middle|\; gh = gh = e$.

Examples of groups:

- $(\mathbb{Z}, +)$
- $(\mathbb{Q}, +)$
- $(\mathbb{Q}^\times, \times)$
- $(\mathbb{R}^\times, \times)$
- $(\mathrm{GL}(n, \mathbb{R}), \times) = \left\{ A \in \mathrm{Mat}_n \;\middle|\; \det(A) \neq 0 \right\}$
- $(S_n, \circ)$

Definition: A subset $S \subseteq G$ is a **subgroup** of G iff

1. **Closure**: $s_1, s_2 \in S \implies s_1 s_2 \in S$
2. **Identity**: $e \in S$
3. **Inverses**: $s \in S \implies s^{-1} \in S$

We denote such a subgroup $S \leq G$.

Examples of subgroups:

- $(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$
- $\mathrm{SL}(n, \mathbb{R}) \leq \mathrm{GL}(n, \mathbb{R})$, where $\mathrm{SL}(n, \mathbb{R}) = \left\{ A \in \mathrm{GL}(n, \mathbb{R}) \;\middle|\; \det(A) = 1 \right\}$

1.3 Cyclic Groups

Definition: A group G is **cyclic** iff G is generated by a single element.

Exercise: Show

$$\langle g \rangle = \left\{ g^n \;\middle|\; n \in \mathbb{Z} \right\} \cong \bigcap_{g \in G} \left\{ H \;\middle|\; H \leq G \text{ and } g \in H \right\}.$$

Theorem: Let G be a cyclic group, so $G = \langle g \rangle$.

- If $|G| = \infty$, then $G \cong \mathbb{Z}$.
- If $|G| = n < \infty$, then $G \cong \mathbb{Z}_n$.

Definition: Let $H \leq G$, and define a **right coset of** G by $aH = \left\{ah \,\middle|\, H \in H\right\}$.

A similar definition can be made for **left cosets**.

Fundamental Theorem of Cosets:

$$aH = bH \iff b^{-1}a \in H \text{ and } Ha = Hb \iff ab^{-1} \in H.$$

Some facts:

- Cosets partition H, i.e.

$$b \notin H \implies aH \bigcap bH = \{e\}.$$

- $|H| = |aH| = |Ha|$ for all $a \in G$.

Theorem (Lagrange): If G is a finite group and $H \leq G$, then $|H| \,\Big|\, |G|$.

Definition A subgroup $N \leq G$ is **normal** iff $gN = Ng$ for all $g \in G$, or equivalently $gNg^{-1} \subseteq N$. (I denote this $N \trianglelefteq G$.)

When $N \trianglelefteq G$, the set of left/right cosets of N themselves have a group structure. So we define

$$G/N = \left\{gN \,\middle|\, g \in G\right\} \text{ where } (g_1N) \cdot (g_2N) \coloneqq (g_1g_2)N.$$

Given $H, K \leq G$, define

$$HK = \left\{hk \,\middle|\, h \in H,\ k \in K\right\}.$$

We have a general formula,

$$|HK| = \frac{|H||K|}{|H \bigcap K|}.$$

1.4 Homomorphisms

Definition: Let G, G' be groups, then $\varphi : G \to G'$ is a **homomorphism** if $\varphi(ab) = \varphi(a)\varphi(b)$.

Examples of homomorphisms:

- $\exp : (\mathbb{R}, +) \to (\mathbb{R}^{>0}, \,\cdot\,)$ since

$$\exp(a+b) \coloneqq e^{a+b} = e^a e^b \coloneqq \exp(a)\exp(b).$$

- $\det : (\mathrm{GL}(n, \mathbb{R}), \times) \to (\mathbb{R}^\times, \times)$ since

$$\det(AB) = \det(A)\det(B).$$

- Let $N \trianglelefteq G$ and define

$$\begin{aligned} \varphi : G &\to G/N \\ g &\mapsto gN. \end{aligned}$$

- Let $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ where $\phi(g) = [g] = g \mod n$ where $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$

Definition: Let $\varphi : G \to G'$. Then φ is a **monomorphism** iff it is injective, an **epimorphism** iff it is surjective, and an **isomorphism** iff it is bijective.

1.5 Direct Products

Let G_1, G_2 be groups, then define

$$G_1 \times G_2 = \left\{ (g_1, g_2) \;\middle|\; g_1 \in G, g_2 \in G_2 \right\} \text{ where } (g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2, h_2).$$

We have the formula $|G_1 \times G_2| = |G_1||G_2|$.

1.6 Finitely Generated Abelian Groups

Definition: We say a group is **abelian** if G is commutative, i.e. $g_1, g_2 \in G \implies g_1 g_2 = g_2 g_1$.

Definition: A group is **finitely generated** if there exist $\{g_1, g_2, \cdots g_n\} \subseteq G$ such that $G = \langle g_1, g_2, \cdots g_n \rangle$.

This generalizes the notion of a cyclic group, where we can simply intersect all of the subgroups that contain the g_i to define it.

We know what cyclic groups look like – they are all isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$. So now we'd like a structure theorem for abelian finitely generated groups.

Theorem: Let G be a finitely generated abelian group.

Then

$$G \cong \mathbb{Z}^r \times \prod_{i=1}^{s} \mathbb{Z}_{p_i^{\alpha_i}}$$

for some finite $r, s \in \mathbb{N}$ where the p_i are (not necessarily distinct) primes.

Example: Let G be a finite abelian group of order 4.

Then $G \cong \mathbb{Z}_4$ or $\mathbb{Z}_2^2$, which are not isomorphic because every element in $\mathbb{Z}_2^2$ has order 2 where $\mathbb{Z}_4$ contains an element of order 4.

1.7 Fundamental Homomorphism Theorem

Let $\varphi : G \to G'$ be a group homomorphism and define

$$\ker \varphi := \left\{ g \in G \;\middle|\; \varphi(g) = e' \right\}.$$

1.7.1 The First Homomorphism Theorem

Theorem: There exists a map $\varphi' : G/\ker\varphi \to G'$ such that the following diagram commutes:

$$\begin{tikzcd}
G \arrow[r, dotted, "\varphi"] \arrow[d, "\eta"'] & G' \\
G/\ker\varphi \arrow[ur, "\varphi'"] &
\end{tikzcd}$$

That is, $\varphi = \varphi' \circ \eta$, and φ' is an isomorphism onto its image, so $G/\ker\varphi = \text{im }\varphi$.

This map is given by

$$\varphi'(g(\ker\varphi)) = \varphi(g).$$

Exercise: Check that φ is well-defined.

1.7.2 The Second Theorem

Theorem: Let $K, N \leq G$ where $N \trianglelefteq G$. Then

$$\frac{K}{N\bigcap K} \cong \frac{NK}{N}$$

Proof: Define a map

$$\begin{aligned}
K &\xrightarrow{\varphi} NK/N \\
k &\mapsto kN.
\end{aligned}$$

You can show that φ is onto, then look at $\ker\varphi$; note that

$$kN = \varphi(k) = N \iff k \in N,$$

and so $\ker\varphi = N\bigcap K$.

$\blacksquare$

2 Tuesday August 20th

2.1 The Fundamental Homomorphism Theorems

Theorem 1: Let $\varphi : G \to G'$ be a homomorphism. Then there is a canonical homomorphism $\eta : G \to G/\ker\varphi$ such that the usual diagram commutes.

Moreover, this map induces an isomorphism $G/\ker\varphi \cong \text{im }\varphi$.

Theorem 2: Let $K, N \leq G$ and suppose $N \trianglelefteq G$. Then there is an isomorphism

$$\frac{K}{K \bigcap N} \cong \frac{NK}{N}$$

Proof Sketch: Show that $K \bigcap N \trianglelefteq G$, and NK is a subgroup exactly because N is normal.

Theorem 3: Let $H, K \trianglelefteq G$ such that $H \leq K$.

Then

1. H/K is normal in G/K.
2. The quotient $(G/K)/(H/K) \cong G/H$.

Proof: We'll use the first theorem.

Define a map

$$\begin{aligned} \phi : G/K &\to G/H \\ gk &\mapsto gH. \end{aligned}$$

Exercise: Show that ϕ is surjective, and that $\ker \phi \cong H/K$.

■

2.2 Permutation Groups

Let A be a set, then a *permutation* on A is a bijective map $A\circlearrowright$. This can be made into a group with a binary operation given by composition of functions. Denote S_A the set of permutations on A.

Theorem: S_A is in fact a group.

Proof: Exercise. Follows from checking associativity, inverses, identity, etc.

■

In the special case that $A = \{1, 2, \cdots n\}$, then $S_n \coloneqq S_A$.

Recall two line notation

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Moreover, $|S_n| = n!$ by a combinatorial counting argument.

Example: S_3 is the symmetries of a triangle.

Example: The symmetries of a square are *not* given by S_4, it is instead D_4.

2.3 Orbits and the Symmetric Group

Permutations S_A *act* on A, and if $\sigma \in S_A$, then $\langle \sigma \rangle$ also acts on A.

Define $a \sim b$ iff there is some n such that $\sigma^n(a) = b$. This is an equivalence relation, and thus induces a partition of A. See notes for diagram. The equivalence classes under this relation are called the *orbits* under σ.

Example:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 6 & 3 & 7 & 4 & 5 & 1 \end{pmatrix} = (18)(2)(364)(57).$$

Definition: A permutation $\sigma \in S_n$ is a *cycle* iff it contains at most one orbit with more than one element.

The *length* of a cycle is the number of elements in the largest orbit.

Recall cycle notation: $\sigma = (\sigma(1)\sigma(2)\cdots\sigma(n))$.

Note that this is read right-to-left by convention!

Theorem: Every permutation $\sigma \in S_n$ can be written as a product of disjoint cycles.

Definition: A *transposition* is a cycle of length 2.

Proposition: Every permutation is a product of transpositions.

Proof:

$$(a_1 a_2 \cdots a_n) = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_2).$$

■

This is not a unique decomposition, however, as e.g. $\mathrm{id} = (12)^2 = (34)^2$.

Theorem: Any $\sigma \in S_n$ can be written as **either**

- An even number of transpositions, or
- An odd number of transpositions.

Proof:

Define

$$A_n = \left\{ \sigma \in S_n \;\middle|\; \sigma \text{ is even} \right\}.$$

We claim that $A_n \trianglelefteq S_n$.

1. Closure: If τ_1, τ_2 are both even, then $\tau_1\tau_2$ also has an even number of transpositions.
2. The identity has an even number of transpositions, since zero is even.
3. Inverses: If $\sigma = \prod_{i=1}^{s} \tau_i$ where s is even, then $\sigma^{-1} = \prod_{i=1}^{s} \tau_{s-i}$. But each τ is order 2, so $\tau^{-1} = \tau$, so there are still an even number of transpositions.

So A_n is a subgroup.

It is normal because it is index 2, or the kernel of a homomorphism, or by a direct computation.

2.4 Groups Acting on Sets

Think of this as a generalization of a G-module.

Definition: A group G is said to *act* on a set X if there exists a map $G \times X \to X$ such that

1. $e \curvearrowright x = x$
2. $(g_1 g_2) \curvearrowright x = g_1 \curvearrowright (g_2 \curvearrowright x)$.

Examples:

1. $G = S_A \curvearrowright A$
2. $H \leq G$, then $G \curvearrowright X = G/H$ where $g \curvearrowright xH = (gx)H$.
3. $G \curvearrowright G$ by conjugation, i.e. $g \curvearrowright x = gxg^{-1}$.

Definition: Let $x \in X$, then define the **stabilizer subgroup**

$$G_x = \left\{ g \in G \;\middle|\; g \curvearrowright x = x \right\} \leq G$$

We can also look at the dual notion,

$$X_g = \left\{ x \in X \;\middle|\; g \curvearrowright x = x \right\}.$$

We then define the *orbit* of an element x as

$$Gx = \left\{ g \curvearrowright x \;\middle|\; g \in G \right\}$$

and we have a similar result where $x \sim y \iff x \in Gy$, and the orbits partition X.

Theorem: Let G act on X. We want to know the number of elements in an orbit, and it turns out that

$$|Gx| = [G : G_x]$$

Proof: Construct a map $Gx \xrightarrow{\psi} G/Gx$ where $\psi(g \curvearrowright x) = gGx$.

Exercise: Show that this is well-defined, so if 2 elements are equal then they go to the same coset.

Exercise: Show that this is surjective.

Injectivity: $\psi(g_1 x) = \psi(g_2 x)$, so $g_1 Gx = g_2 Gx$ and $(g_2^{-1} g_1) Gx = Gx$ so

$$g_2^{-1} g_1 \in Gx \iff g_2^{-1} g_1 \curvearrowright x = x \iff g_1 x = g_2 x.$$

■

Next time: Burnside's theorem, proving the Sylow theorems.

3 Thursday August 22nd

3.1 Group Actions

Let G be a group and X be a set; we say G *acts* on X (or that X is a G- set) when there is a map $G \times X \to X$ such that $ex = x$ and

$$(gh) \curvearrowright x = g \curvearrowright (h \curvearrowright x).$$

We then define the **stabilizer** of x as

$$\mathrm{Stab}_G(x) = G_x \coloneqq \left\{ g \in G \;\middle|\; g \curvearrowright x = x \right\} \leq G,$$

and the **orbit**

$$G.x = \mathcal{O}_x \coloneqq \left\{ g \curvearrowright x \;\middle|\; x \in X \right\} \subseteq X.$$

When G is finite, we have

$$|G.x| = \frac{|G|}{|G_x|}.$$

We can also consider the **fixed points** of X,

$$X_g = \left\{ x \in X \;\middle|\; g \curvearrowright x = x \; \forall g \in G \right\} \subseteq X$$

3.2 Burnside's Theorem

Theorem (Burnside): Let X be a G-set and $v \coloneqq |X/G|$ be the number of orbits. Then

$$v|G| = \sum_{g \in G} |X_g|.$$

Proof: Define

$$N = \left\{ (g, x) \;\middle|\; g \curvearrowright x = x \right\} \subseteq G \times X,$$

we then have

$$
\begin{aligned}
|N| &= \sum_{g \in G} |X_g| \\
&= \sum_{x \in X} |G_x| \\
&= \sum_{x \in X} \frac{|G|}{|G.x|} \quad \text{by Orbit-Stabilizer} \\
&= |G| \left(\sum_{x \in X} \frac{1}{|G.x|} \right) \\
&= |G| \sum_{G.x \ \in \ X/G} \left(\sum_{y \ \in \ G.x} \frac{1}{|G.x|} \right) \\
&= |G| \sum_{G.x \ \in \ X/G} \left(|G.x| \frac{1}{|G.x|} \right) \\
&= |G| \sum_{G.x \ \in \ X/G} 1 \\
&= |G| v.
\end{aligned}
$$

The last two equalities follow from the following fact: since the orbits partition X, say into $X = \coprod_{i=1}^{v} \sigma_i$, so let $\sigma = \left\{ \sigma_i \,\middle|\, 1 \leq i \leq v \right\}$.

By abuse of notation, replace each orbit in σ with a representative element $x_i \in \sigma_i \subset X$.

We then have

$$
\sum_{x \in \sigma} \frac{1}{|G.x|} = \frac{1}{|G.x|} |\sigma| = 1.
$$

■

Application: Consider seating 10 people around a circular table. How many distinct seating arrangements are there?

Let X be the set of configurations, $G = S_{10}$, and let $G \curvearrowright X$ by permuting configurations. Then v, the number of orbits under this action, yields the number of distinct seating arrangements.

By Burnside, we have

$$
v = \frac{1}{|G|} \sum_{g \in G} |X_g| = \frac{1}{10}(10!) = 9!
$$

since $X_g = \left\{ x \in X \,\middle|\, g \curvearrowright x = x \right\} = \emptyset$ unless $g = e$, and $X_e = X$.

3.3 Sylow Theory

Recall Lagrange's theorem:

If $H \leq G$ and G is finite, then $|H|$ divides $|G|$.

Consider the converse: if n divides $|G|$, does there exist a subgroup of size n?

The answer is **no** in general, and a counterexample is A_4 which has $4!/2 = 12$ elements but no subgroup of order 6.

3.3.1 Class Functions

Let X be a G-set, and choose orbit representatives $x_1 \cdots x_v$.

Then

$$|X| = \sum_{i=1}^{v} |G.x_i|.$$

We can then separately count all orbits with exactly one element, which is exactly

$$X_G = \left\{ x \in G \;\middle|\; g \curvearrowright x = x \;\forall g \in G \right\}$$

.

We then have

$$|X| = |X_G| + \sum_{i=j}^{v} |G.x_i|$$

for some j where $|G.x_i| > 1$ for all $i \geq j$.

Theorem: Let G be a group of order p^n for p a prime.

Then

$$|X| = |X_G| \mod p.$$

Proof: We know that

$$|G.x_i| = [G : G_{x_i}] \text{ for } j \leq i \leq v \text{ and } |Gx_i| > 1 \implies G.x_i \neq G,$$

and thus p divides $[G : Gx_i]$. The result follows.

■

Application: If $|G| = p^n$, then the center $Z(G)$ is nontrivial.

Let $X = G$ act on itself by conjugation, so $g \curvearrowright x = gxg^{-1}$. Then

$$X_G = \left\{ x \in G \;\middle|\; gxg^{-1} = x \right\} = \left\{ x \in G \;\middle|\; gx = xg \right\} = Z(G)$$

But then, by the previous theorem, we have

$$|Z(G)| \equiv |X| \equiv |G| \mod p,$$

but since $Z(G) \leq G$ we have $|Z(G)| \cong 0 \mod p$. So in particular, $Z(G) \neq \{e\}$.

Definition: A group G is a p**-group** iff every element in G has order p^k for some k. A subgroup is a p-group exactly when it is a p-group in its own right.

3.3.2 Cauchy's Theorem

Theorem (Cauchy): Let G be a finite group, where p is prime and divides $|G|$. Then G has an element (and thus a subgroup) of order p.

Proof: Consider

$$X = \left\{ (g_1, g_2, \cdots, g_p) \in G^{\oplus p} \;\middle|\; g_1 g_2 \cdots g_p = e \right\}.$$

Given any $p-1$ elements, say $g_1 \cdots g_{p-1}$, the remaining element is completely determined by $g_p = (g_1 \cdots g_{p-1})^{-1}$.

So $|X| = |G|^{p-1}$.and since $p \;\Big|\; |G|$, we have $p \;\Big|\; |X|$.

Now let $\sigma \in S_p$ the symmetric group act on X by index permutation, i.e.

$$\sigma \curvearrowright (g_1, g_2 \cdots g_p) = (g_{\sigma(1)}, g_{\sigma(2)}, \cdots, g_{\sigma(p)}).$$

Exercise: Check that this gives a well-defined group action.

Let $\sigma = (1\ 2\ \cdots\ p) \in S_p$, and note $\langle \sigma \rangle \leq S_p$ also acts on X where $|\langle \sigma \rangle| = p$. Therefore we have

$$|X| = \left| X_{\langle \sigma \rangle} \right| \mod p.$$

Since $p \;\Big|\; |X|$, it follows that $\left| X_{\langle \sigma \rangle} \right| = 0 \mod p$, and thus $p \;\Big|\; \left| X_{\langle \sigma \rangle} \right|$.

If $\langle \sigma \rangle$ fixes $(g_1, g_2, \cdots g_p)$, then $g_1 = g_2 = \cdots g_p$.

Note that $(e, e, \cdots) \in X_{\langle \sigma \rangle}$, as is $(a, a, \cdots a)$ since $p \;\Big|\; \left| X_{\langle \sigma \rangle} \right|$. So there is some $a \in G$ such that $a^p = 1$. Moreover, $\langle a \rangle \leq G$ is a subgroup of size p.

■

3.3.3 Normalizers

Let G be a group and $X = S$ be the set of subgroups of G. Let G act on X by $g \curvearrowright H = gHg^{-1}$. What is the stabilizer?

$$G_x = G_H = \left\{ g \in G \;\middle|\; gHg^{-1} = H \right\},$$

making G_H the largest subgroup such that $H \trianglelefteq G_H$.

So we **define** $N_G(H) \coloneqq G_H$.

Lemma: Let H be a p-subgroup of G of order p^n. Then

$$[N_G(H) : H] = [G : H] \mod p.$$

Proof: Let $S = G/H$ be the set of left H-cosets in G. Now let H act on S by

$$H \curvearrowright x + H \coloneqq (hx) + H.$$

By a previous theorem, $|G/H| = |S| = |S_H| \mod p$, where $|G/H| = [G : H]$. What is S_H?

This is given by

$$S_H = \left\{ x + H \in S \,\middle|\, xHx^{-1} \in H \forall h \in H \right\}.$$

Therefore $x \in N_G(H)$.

■

Corollary: Let $H \leq G$ be a subgroup of order p^n. If $p \,\middle|\, [G : H]$ then $N_G(H) \neq H$.

Proof: Exercise. ■

Theorem: Let G be a finite group, then G is a p-group $\iff$ $|G| = p^n$ for some $n \geq 1$.

Proof: Suppose $|G| = p^n$ and $a \in G$. Then $|\langle a \rangle| = p^\alpha$ for some α.

Conversely, suppose G is a p-group. Factor $|G|$ into primes and suppose $\exists q$ such that $q \,\middle|\, |G|$ but $q \neq p$.

By Cauchy, we can then get a subgroup $\langle c \rangle$ such that $|\langle c \rangle| \,\middle|\, q$, but then $|G| \neq p^n$.

■

4 Tuesday August 27th

Let G be a finite group and p a prime. TFAE:

- $|H| = p^n$ for some n
- Every element of H has order p^α for some α.

If either of these are true, we say H is a *p-group*.

Let H be a p-group, last time we proved that if $p \,\middle|\, [G : H]$ then $N_G(H) \neq H$.

4.1 Sylow Theorems

Let G be a finite group and suppose $|G| = p^n m$ where $(m, n) = 1$. Then

4.1.1 Sylow 1

> Idea: take a prime factorization of $|G|$, then there are subgroups of order p^i for *every* prime power appearing, up to the maximal power.

1. G contains a subgroup of order p^i for every $1 \leq i \leq n$.
2. Every subgroup H of order p^i where $i < n$ is a normal subgroup in a subgroup of order p^{i+1}.

Proof: By induction on i. For $i = 1$, we know this by Cauchy's theorem. If we show (2), that shows (1) as a consequence.

So suppose this holds for $i < n$. Let $H \leq G$ where $|H| = p^i$, we now want a subgroup of order p^{i+1}. Since $p \,\Big|\, [G : H]$, by the previous theorem, $H < N_G(H)$ is a proper subgroup (?).

Now consider the canonical projection $N_G(H) \to N_G(H)/H$. Since

$$p \,\Big|\, [N_G(H) : H] = |N_G(H)/H|,$$

by Cauchy there is a subgroup of order p in this quotient. Call it K. Then $\pi^{-1}(K) \leq N_G(H)$.

Exercise: Show that $\left|\phi^{-1}(K)\right| = p^{i+1}$.

It now follows that $H \trianglelefteq \phi^{-1}(K)$. ■

Definition: For G a finite group and $|G| = p^n m$ where p does not divide m.

Then a subgroup of order p^n is called a **Sylow p-subgroup**.

Note: by Sylow 1, these exist.

4.1.2 Sylow 2

If P_1, P_2 are Sylow p-subgroups of G, then P_1 and P_2 are conjugate.

Proof: Let $\mathcal{L}$ be the left cosets of P_1, i.e. $\mathcal{L} = G/P_1$.

Let P_2 act on $\mathcal{L}$ by

$$p_2 \curvearrowright (g + P_1) \coloneqq (p_2 g) + P_1.$$

By a previous theorem about orbits and fixed points, we have

$$|\mathcal{L}_{P_2}| = |\mathcal{L}| \mod p.$$

Since p does not divide $|\mathcal{L}|$, we have p does not divide $|\mathcal{L}_{P_2}|$. So $\mathcal{L}_{P_2}$ is nonempty.

So there exists a coset xP_1 such that $xP_1 \in \mathcal{L}_{P_2}$, and thus

$$yxP_1 = xP_1 \text{ for all } y \in P_2.$$

Then $x^{-1}yxP_1 = P_1$ for all $y \in P_2$, and so $x^{-1}P_2x = P_1$. So P_1 and P_2 are conjugate.

■

4.1.3 Sylow 3

Let G be a finite group, and $p \,\Big|\, |G|$. Let r_p be the number of Sylow p-subgroups of G.

Then

- $r_p \cong 1 \mod p$.
- $r_p \,\Big|\, |G|$.

- $r_p = [G : N_G(P)]$

Proof:

Let $X = \mathcal{S}$ be the set of Sylow p-subgroups, and let $P \in X$ be a fixed Sylow p-subgroup.

Let $P \curvearrowright \mathcal{S}$ by conjugation, so for $\overline{P} \in \mathcal{S}$ let $x \curvearrowright \overline{P} = x\overline{P}x^{-1}$.

By a previous theorem, we have

$$|\mathcal{S}| = \mathcal{S}_P \mod p$$

What are the fixed points $\mathcal{S}_P$?

$$\mathcal{S}_P = \left\{ T \in \mathcal{S} \;\middle|\; xTx^{-1} = T \quad \forall x \in P \right\}.$$

Let $\mathcal{T} \in \mathcal{S}_P$, so $xTx^{-1} = T$ for all $x \in P$.

Then $P \leq N_G(T)$, so both P and T are Sylow p- subgroups in $N_G(H)$ as well as G.

So there exists a $f \in N_G(T)$ such that $T = gPg^{-1}$. But the point is that in the normalizer, there is only **one** Sylow p- subgroup.

But then T is the unique largest normal subgroup of $N_G(T)$, which forces $T = P$.

Then $\mathcal{S}_P = \{P\}$, and using the formula, we have $r_p \cong 1 \mod p$.

Now modify this slightly by letting G act on $\mathcal{S}$ (instead of just P) by conjugation.

Since all Sylows are conjugate, by Sylow (1) there is only one orbit, so $\mathcal{S} = GP$ for $P \in \mathcal{S}$. But then

$$r_p = |\mathcal{S}| = |GP| = [G : G_p] \;\Big|\; |G|.$$

Note that this gives a precise formula for r_p, although the theorem is just an upper bound of sorts, and $G_p = N_G(P)$.

4.2 Applications of Sylow Theorems

Of interest historically: classifying finite *simple* groups, where a group G is *simple* If $N \trianglelefteq G$ and $N \neq \{e\}$, then $N = G$.

Example: Let $G = \mathbb{Z}_p$, any subgroup would need to have order dividing p, so G must be simple.

Example: $G = A_n$ for $n \geq 5$ (see Galois theory)

One major application is proving that groups of a certain order are *not* simple.

Applications:

Proposition: Let $|G| = p^n q$ with $p > q$. Then G is not simple.

Proof:

> Strategy: Find a proper normal nontrivial subgroup using Sylow theory. Can either show $r_p = 1$, or produce normal subgroups by intersecting distinct Sylow p-subgroups.

Consider r_p, then $r_p = p^\alpha q^\beta$ for some α, β. But since $r_p \cong 1 \mod p$, p does not divide r_p, we must have $r_p = 1, q$.

But since $q < p$ and $q \neq 1 \mod p$, this forces $r_p = 1$.

So let P be a sylow p-subgroup, then $P < G$. Then gPg^{-1} is also a sylow, but there's only 1 of them, so P is normal.

$\blacksquare$

Proposition: Let $|G| = 45$, then G is not simple.

Proof: Exercise.

$\blacksquare$

Proposition: Let $|G| = p^n$, then G is not simple if $n > 1$.

Proof: By Sylow (1), there is a normal subgroup of order p^{n-1} in G.

$\blacksquare$

Proposition: Let $|G| = 48$, then G is not simple.

Proof:

Note $48 = 2^4 3$, so consider r_2, the number of Sylow 2-subgroups. Then $r_2 \cong 1 \mod 2$ and $r_2 \,\Big|\, 48$. So $r_2 = 1, 3$. If $r_2 = 1$, we're done, otherwise suppose $r_2 = 3$.

Let $H \neq K$ be Sylow 2-subgroups, so $|H| = |K| = 2^4 = 16$. Now consider $H \bigcap K$, which is a subgroup of G. How big is it?

Since $H \neq K$, $\left|H \bigcap K\right| < 16$. The order has to divides 16, so we in fact have $\left|H \bigcap K\right| \leq 8$. Suppose it is less than 4, towards a contradiction. Then

$$|HK| = \frac{|H||K|}{|H \bigcap K|} \geq \frac{(16)(16)}{4} = 64 > |G| = 48.$$

So we can only have $\left|H \bigcap K\right| = 8$. Since this is an index 2 subgroup in both H and K, it is in fact normal. But then

$$H, K \subseteq N_G(H \bigcap K) \coloneqq X.$$

But then $|X|$ must be a multiple of 16 *and* divide 48, so it's either 16 or 28. But $|X| > 16$, because $H \subseteq X$ and $K \subseteq X$. So then

$$N_G(H \bigcap K) = G \text{ and so } H \bigcap K \trianglelefteq G.$$

$\blacksquare$

5 Thursday August 29th

5.1 Classification of Groups of Certain Orders

We have a classification of some finite abelian groups.

Order of G	Number of Groups	List of Distinct Groups
1	1	$\{e\}$
2	1	$\mathbb{Z}_2$
3	1	$\mathbb{Z}_3$
4	2	$\mathbb{Z}_4, \mathbb{Z}_2^2$
5	1	$\mathbb{Z}_5$
6	2	$\mathbb{Z}_6, S_3$ (*)
7	1	$\mathbb{Z}_7$
8	5	$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2^3, D_4, Q$
9	2	$\mathbb{Z}_9, \mathbb{Z}_3^2$
10	2	$\mathbb{Z}_{10}, D_5$
11	1	$\mathbb{Z}_{11}$

Exercise: show that groups of order p^2 are abelian.

We still need to justify S_3, D_4, Q, D_5.

Recall that for any group A, we can consider the free group on the elements of A given by $F[A]$.

Note that we can also restrict A to just its generators.

There is then a homomorphism $F[A] \to A$, where the kernel is the relations.

Example:

$$\mathbb{Z} * \mathbb{Z} = \left\langle x, y \;\middle|\; xyx^{-1}y^{-1} = e \right\rangle \text{ where } x = (1,0),\ y = (0,1).$$

5.2 Groups of Order 6

Let G be nonabelian of order 6.

Idea: look at subgroups of index 2.

Let P be a Sylow 3-subgroup of G, then $r_3 = 1$ so $P \trianglelefteq G$. Moreover, P is cyclic since it is order 3, so $P = \langle a \rangle$.

But since $|G/P| = 2$, it is also cyclic, so $G/P = \langle bP \rangle$.

Note that $b \notin P$, but $b^2 \in P$ since $(bP)^2 = P$, so $b^2 \in \left\{e, a, a^2\right\}$.

If $b = a, a^2$ then b has order 6, but this would make $G = \langle b \rangle$ cyclic and thus abelian. So $b^2 = 1$.

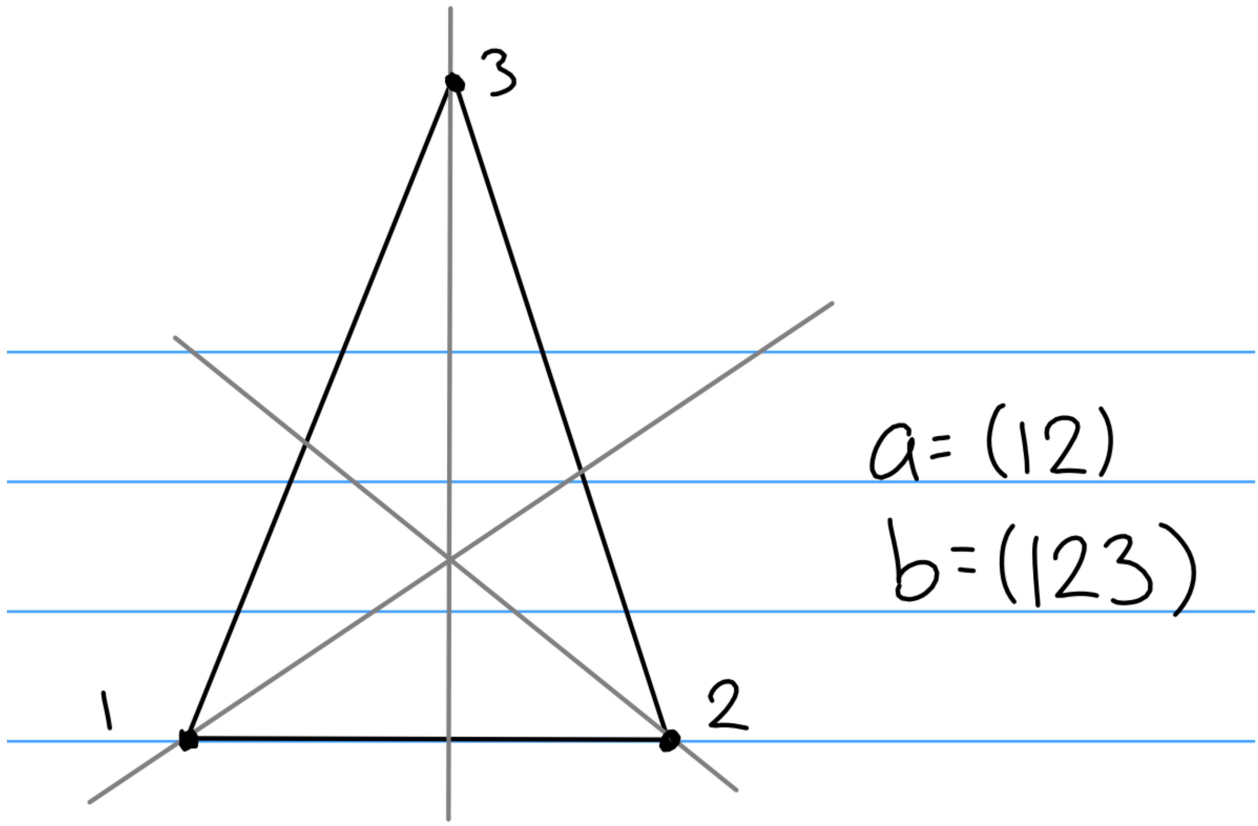
Since $P \trianglelefteq G$, we have $bPb^{-1} = P$, and in particular bab^{-1} has order 3.

So either $bab^{-1} = a$, or $bab^{-1} = a^2$. If $bab^{-1} = a$, then G is abelian, so $bab^{-1} = a^2$. So

$$G = \left\langle a, b \;\middle|\; a^3 = e, b^2 = e, bab^{-1} = a^2 \right\rangle.$$

We've shown that *if* there is such a nonabelian group, then it must satisfy these relations – we still need to produce some group that actually realizes this.

Consider the symmetries of the triangle:



You can check that a, b satisfy the appropriate relations.

5.3 Groups of Order 10

For order 10, a similar argument yields

$$G = \left\langle a, b \;\middle|\; a^5 = 1, b^2 = 1, ba = a^4 b \right\rangle,$$

and this is realized by symmetries of the pentagon where $a = (1\ 2\ 3\ 4\ 5), b = (1\ 4)(2\ 3)$.

5.4 Groups of Order 8

Assume G is nonabelian of order 8. G has no elements of order 8, so the only possibilities for orders of elements are 1, 2, or 4.

Assume all elements have order 1 or 2. Let $a, b \in G$, consider

$$(ab)^2 = abab \implies ab = b^{-1}a^{-1} = ba,$$

and thus G is abelian. So there must be an element of order 4.

So suppose $a \in G$ has order 4, which is an index 2 subgroup, and so $\langle a \rangle \trianglelefteq G$.

But $|G/\langle a\rangle| = 2$ is cyclic, so $G/\langle a\rangle = \langle bH\rangle$.

Note that $b^2 \in H = \langle a\rangle$.

If $b^2 = a, a^3$ then b will have order 8, making G cyclic. So $b^2 = 1, a^2$. These are both valid possibilities.

Since $H \trianglelefteq G$, we have $b\langle a\rangle b^{-1} = \langle a\rangle$, and since a has order 4, so does bab^{-1}.

So $bab^{-1} = a, a^3$, but a is not an option because this would make G abelian.

So we have two options:

$$\begin{aligned} G_1 &= \left\langle a, b \;\middle|\; a^4 = 1, b^2 = 1, bab^{-1} = a^3 \right\rangle \\ G_2 &= \left\langle a, b \;\middle|\; a^4 = 1, b^2 = a^2, bab^{-1} = a^3 \right\rangle. \end{aligned}$$

Exercise: prove $G_1 \ncong G_2$.

Now to realize these groups:

- G_1 is the group of symmetries of the square, where $a = (1\ 2\ 3\ 4), b = (1\ 3)$.
- $G_2 \cong Q$, the quaternions, where $Q = \{\pm 1, \pm i, \pm j, \pm k\}$, and there are relations (add picture here).

5.5 Some Nice Facts

- If and $\phi : G \to G'$, then
  - $N \trianglelefteq G \implies N \trianglelefteq \phi(G)$, although it is not necessarily normal in G.
  - $N' \trianglelefteq G' \implies \phi^{-1}(N') \trianglelefteq G$

Definition: A *maximal normal subgroup* is a normal subgroup $M \trianglelefteq G$ that is properly contained in G, and if $M \leq N \trianglelefteq G$ (where N is proper) then $M = N$.

Theorem: M is a maximal normal subgroup of G iff G/M is simple.

5.6 Simple Groups

Definition: A group G is simple iff $N \trianglelefteq G \implies N = \{e\}, G$.

Note that if an abelian group has *any* subgroups, then it is not simple, so $G = \mathbb{Z}_p$ is the only simple abelian group. Another example of a simple group is A_n for $n \geq 5$.

Theorem (Feit-Thompson, 1964): Every finite nonabelian simple group has even order.

Note that this is a consequence of the "odd order theorem".

5.7 Series of Groups

A composition series is a descending series of pairwise normal subgroups such that each successive quotient is simple:

$$\begin{aligned} G_0 \trianglelefteq G_1 \trianglelefteq G_2 \cdots &\trianglelefteq \{e\} \\ G_i/G_{i+1} &\text{ simple.} \end{aligned}$$

Example:

$$\begin{aligned} \mathbb{Z}_9 \trianglelefteq \mathbb{Z}_3 \trianglelefteq \{e\} \\ \mathbb{Z}_9/\mathbb{Z}_3 = \mathbb{Z}_3, \\ \mathbb{Z}_3/\{e\} = \mathbb{Z}_3. \end{aligned}$$

Example:

$$\begin{aligned} \mathbb{Z}_6 \trianglelefteq \mathbb{Z}_3 \trianglelefteq \{e\} \\ \mathbb{Z}_6/\mathbb{Z}_3 = \mathbb{Z}_2 \\ \mathbb{Z}_2/\{e\} = \mathbb{Z}_2. \end{aligned}$$

but also

$$\begin{aligned} \mathbb{Z}_6 \trianglelefteq \mathbb{Z}_2 \trianglelefteq \{e\} \\ \mathbb{Z}_6/\mathbb{Z}_2 = \mathbb{Z}_3 \\ \mathbb{Z}_3/\{e\} = \mathbb{Z}_3. \end{aligned}$$

Theorem (Jordan-Holder): Any two composition series are "isomorphic" in the sense that the same quotients appear in both series, up to a permutation.

Definition: A group is *solvable* iff it has a composition series where all factors are abelian.

Exercise: Show that any abelian group is solvable.

Example: S_n is *not* solvable for $n \geq 5$, since

$$\begin{aligned} S_n \trianglelefteq A_n \trianglelefteq \{e\} \\ S_n/A_n = \mathbb{Z}_2 \text{ simple} \\ A_n/\{e\} = A_n \text{ simple } \iff n \geq 5. \end{aligned}$$

Example:

$$
\begin{aligned}
S_4 \trianglelefteq A_4 \trianglelefteq G \trianglelefteq \{e\} \quad &\text{where } |H| = 4 \\
S_4/A_4 &= \mathbb{Z}_2 \\
A_4/H &= \mathbb{Z}_3 \\
H/\{e\} &= \{a, b\}?.
\end{aligned}
$$

6 August 30th

Recall the Sylow theorems:

- p groups exist for *every* p^i dividing $|G|$, and $H(p) \trianglelefteq H(p^2) \trianglelefteq \cdots H(p^n)$.
- All Sylow p-subgroups are conjugate.
- Numerical constraints
  - $r_p \cong 1 \mod p$,
  - $r_p \Bigm| |G|$ and $r_p \Bigm| m$,

6.1 Internal Direct Products

Suppose $H, K \leq G$, and consider the smallest subgroup containing both H and K. Denote this $H \vee K$.

If either H or K is normal in G, then we have $H \vee K = HK$.

There is a "recipe" for proving you have a direct product of groups:

Theorem (Recognizing Direct Products): Let G be a group, $H \trianglelefteq G$ and $K \trianglelefteq G$, and

1. $H \vee K = HK = G$,
2. $H \bigcap K = \{e\}$.

Then $G \cong H \times K$.

Proof: We first want to show that $hk = kh \; \forall k \in K, h \in H$. We then have

$$hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K = h(kh^{-1}k^{-1}) \in H \implies hkh^{-1}k^{-1} \in H \bigcap K = \{e\}.$$

So define

$$
\begin{aligned}
\phi : H \times K &\to G \\
(h, k) &\mapsto hk,
\end{aligned}
$$

Exercise: check that this is a homomorphism, it is surjective, and injective.

■

Applications:

Theorem: Every group of order p^2 is abelian.

Proof: If G is cyclic, then it is abelian and $G \cong \mathbb{Z}_{p^2}$. So suppose otherwise. By Cauchy, there is an element of order p in G. So let $H = \langle a \rangle$, for which we have $|H| = p$.

Then $H \trianglelefteq G$ by Sylow 1, since it's normal in $H(p^2)$, which would have to equal G.

Now consider $b \notin H$. By Lagrange, we must have $o(b) = 1, p$, and since $e \in H$, we must have $o(b) = p$. This uses fact that G is not cyclic.

Now let $K = \langle b \rangle$. Then $|K| = p$, and $K \trianglelefteq G$ by the same argument.

■

Theorem: Let $|G| = pq$ where $q \neq 1 \mod p$ and $p < q$. Then G is cyclic (and thus abelian).

Proof: Use Sylow 1. Let P be a sylow p-subgroup. We want to show that $P \trianglelefteq G$ to apply our direct product lemma, so it suffices to show $r_p = 1$.

We know $r_p = 1 \mod p$ and $r_p \,\Big|\, |G| = pq$, and so $r_p = 1, q$. It can't be q because $p < q$.

Now let Q be a sylow q-subgroup. Then $r_q \cong 1 \mod 1$ and $r_q \,\Big|\, pq$, so $r_q = 1, q$. But since $p < q$, we must have $r_q = 1$. So $Q \trianglelefteq G$ as well.

We now have $P \bigcap Q = \emptyset$ (why?) and

$$|PQ| = \frac{|P||Q|}{|P \bigcap Q|} = |P||Q| = pq,$$

and so $G = PQ$, and $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

■

Example: Every group of order $15 = 5^1 3^1$ is cyclic.

6.2 Determination of groups of a given order

Order of G	Number of Groups	List of Distinct Groups
1	1	$\{e\}$
2	1	$\mathbb{Z}_2$
3	1	$\mathbb{Z}_3$
4	2	$\mathbb{Z}_4, \mathbb{Z}_2^2$
5	1	$\mathbb{Z}_5$
6	2	$\mathbb{Z}_6, S_3$ (*)
7	1	$\mathbb{Z}_7$
8	5	$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2^3, D_8, Q$
9	2	$\mathbb{Z}_9, \mathbb{Z}_3^2$
10	2	$\mathbb{Z}_{10}, D_5$
11	1	$\mathbb{Z}_{11}$

We still need to justify 6, 8, and 10.

6.3 Free Groups

Define an *alphabet* $A = \{a_1, a_2, \cdots a_n\}$, and let a *syllable* be of the form a_i^m for some m. A *word* is any expression of the form $\prod_{n_i} a_{n_i}^{m_i}$.

We have two operations,

- Concatenation, i.e. $(a_1a_2) \star (a_3^2a_5) = a_1a_2a_3^2a_5$.
- Contraction, i.e. $(a_1a_2^2) \star (a_2^{-1}a_5) = a_1a_2^2a_2^{-1}a_5 = a_1a_2a_5$.

If we've contracted a word as much as possible, we say it is *reduced.*

We let $F[A]$ be the set of reduced words and define a binary operation

$$
\begin{aligned}
f : F[A] \times F[A] &\to F[A] \\
(w_1, w_2) &\mapsto w_1w_2 \text{ (reduced)} .
\end{aligned}
$$

Theorem: (A, f) is a group.

Proof: Exercise.

$\blacksquare$

Definition: $F[A]$ is called the **free group generated by** A. A group G is called *free* on a subset $A \subseteq G$ iff $G \cong F[A]$.

Examples:

1. $A = \{x\} \implies F[A] = \left\{x^n \;\middle|\; n \in \mathbb{Z}\right\} \cong \mathbb{Z}$.
2. $A = \{x, y\} \implies F[A] = \mathbb{Z} * \mathbb{Z}$ (not defined yet!).

Note that there are not relations, i.e. $xyxyxy$ is *reduced.* To abelianize, we'd need to introduce the relation $xy = yx$.

Properties:

1. If G is free on A and free on B then we must have $|A| = |B|$.
2. Any (nontrivial) subgroup of a free group is free.

   (See Fraleigh or Hungerford for possible Algebraic proofs!)

Theorem: Let G be generated by some (possibly infinite) subset $A = \left\{A_i \;\middle|\; i \in I\right\}$ and G' be generated by some $A_i' \subseteq A_i$.

Then

a. There is at most one homomorphism $a_i \to a_i'$.

b. If $G \cong F[A]$, there is exactly *one* homomorphism.

Corollary: Every group G' is a homomorphic image of a free group.

Proof: Let A be the generators of G' and $G = F[A]$, then define

$$\begin{aligned} \phi : F[A] &\to G' \\ a_i &\mapsto a_i. \end{aligned}$$

This is onto exactly because $G' = \langle a_i \rangle$, and using the theorem above we're done.

■

6.4 Generators and Relations

Let G be a group and $A \subseteq G$ be a generating subset so $G = \left\langle a \;\middle|\; a \in A \right\rangle$. There exists a $\phi : F[A] \twoheadrightarrow G$, and by the first isomorphism theorem, we have $F[A]/\ker\phi \cong G$.

Let $R = \ker\phi$, these provide the *relations*.

Examples:

Let $G = \mathbb{Z}_3 = \langle [1]_3 \rangle$. Let $x = [1]_3$, then define $\phi : F[\{x\}] \twoheadrightarrow \mathbb{Z}_3$.

Then since $[1] + [1] + [1] = [0] \mod 3$, we have $\ker\phi = \left\langle x^3 \right\rangle$.

Let $G = \mathbb{Z} \oplus \mathbb{Z}$, then $G \cong \left\langle x, y \;\middle|\; [x, y] = 1 \right\rangle$.

> We'll use this for groups of order 6 – there will be only one presentation that is nonabelian, and we'll exhibit such a group.

7 September 9th

7.1 Series of Groups

Recall that a *simple* group has no nontrivial normal subgroups.

Example:

$$\begin{aligned} \mathbb{Z}_6 \trianglelefteq \langle [3] \rangle &\trianglelefteq \langle [0] \rangle \\ \mathbb{Z}_6 / \langle [3] \rangle &= \mathbb{Z}_3 \\ \langle [3] \rangle / \langle [0] \rangle &= \mathbb{Z}_2. \end{aligned}$$

Definition: A *normal series* (or an *invariant series*) of a group G is a finite sequence $H_i \leq G$ such that $H_i \trianglelefteq H_{i+1}$ and $H_n = G$, so we obtain

$$H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_n = G.$$

Definition: A normal series $\{K_i\}$ is a **refinement** of $\{H_i\}$ if $K_i \leq H_i$ for each i.

Definition: We say two normal series of the same group G are *isomorphic* if there is a bijection from

$$\{H_i/H_{i+1}\} \iff \{K_j/K_{j+1}\}$$

Theorem (Schreier): Any two normal series of G has isomorphic refinements.

Definition: A normal series of G is a **composition series** iff all of the successive quotients H_i/H_{i+1} are **simple**.

Note that every finite group has a composition series, because any group is a maximal normal subgroup of itself.

Theorem (Jordan-Holder): Any two composition series of a group G are isomorphic.

Proof: Apply Schreier's refinement theorem.

$\blacksquare$

Example: Consider $S_n \trianglelefteq A_n \trianglelefteq \{e\}$. This is a composition series, with quotients Z_2, A_n, which are both simple.

Definition: A group G is **solvable** iff it has a composition series in which all of the successive quotients are **abelian**.

Examples:

- Any abelian group is solvable.
- S_n is not solvable for $n \geq 5$, since A_n is not abelian for $n \geq 5$.

Recall Feit-Thompson: Any nonabelian simple group is of *even* order.

Consequence: Every group of *odd* order is solvable.

7.2 The Commutator Subgroup

Let G be a group, and let $[G, G] \leq G$ be the subgroup of G generated by elements $aba^{-1}b^{-1}$, i.e. every element is a *product* of commutators. So $[G, G]$ is called *the commutator subgroup.*

Theorem: Let G be a group, then

1. $[G, G] \leq G$
2. $[G, G]$ is a normal subgroup
3. $G/[G, G]$ is abelian.
4. $[G, G]$ is the smallest normal subgroup such that the quotient is abelian,

   I.e., $H \trianglelefteq G$ and if G/N is abelian $\implies [G, G] \leq N$.

Proof of 1:

$[G, G]$ is a subgroup:

- Closure is clear from definition as generators.
- The identity is $e = ee^{-1}ee^{-1}$.

- So it suffices to show that $(aba^{-1}b^{-1})^{-1} \in [G,G]$, but this is given by $bab^{-1}a^{-1}$ which is of the correct form.

$\blacksquare$

Proof of 2:

$[G,G]$ is normal.

Let $x_i \in [G,G]$, then we want to show $g\prod x_i g^{-1} \in [G,G]$, but this reduces to just showing $gxg^{-1} \in [G,G]$ for a single $x \in [G,G]$.

Then,

$$\begin{aligned} g(aba^{-1}b^{-1})g^{-1} &= (g^{-1}aba^{-1})e(b^{-1}g) \\ &= (g^{-1}aba^{-1})(gb^{-1}bg^{-1})(b^{-1}g) \\ &= [(g^{-1}a)b(g^{-1}a)^{-1}b^{-1}][bg^{-1}b^{-1}g] \\ &\in [G,G]. \end{aligned}$$

$\blacksquare$

Proof of 3:

$G/[G,G]$ is abelian.

Let $H = [G,G]$. We have $aHbH = (ab)H$ and $bHaH = (ba)H$.

But $abH = baH$ because $(ba)^{-1}(ab) = a^{-1}b^{-1}ab \in [G,G]$.

$\blacksquare$

Proof of 4:

$H \trianglelefteq G$ and if G/N is abelian $\implies [G,G] \leq N$.

Suppose G/N is abelian. Let $aba^{-1}b^{-1} \in [G,G]$.

Then $abN = baN$, so $aba^{-1}b^{-1} \in N$ and thus $[G,G] \subseteq N$.

$\blacksquare$

7.3 Free Abelian Groups

Example: $\mathbb{Z} \times \mathbb{Z}$.

Take $e_1 = (1,0), e_2 = (0,1)$. Then $(x,y) \in \mathbb{Z}^2$ can be written $x(1,0) + y(0,1)$, so $\{e_i\}$ behaves like a basis for a vector space.

Definition: A group G is *free abelian* if there is a subset $X \subseteq G$ such that every $g \in G$ can be represented as

$$g = \sum_{i=1}^{r} n_i x_i, \quad x_i \in X,\ n_i \in \mathbb{Z}.$$

Equivalently, X generates G, so $G = \langle X \rangle$, and if $\sum n_i x_i = 0 \implies n_i = 0 \; \forall i$.

If this is the case, we say X is a **basis** for G.

Examples:

- $\mathbb{Z}^n$ is free abelian
- $\mathbb{Z}_n$ is not free abelian, since $n[1] = 0$ and $n \neq 0$.

> In general, you can replace $\mathbb{Z}_n$ by any finite group and replace n with the order of the group.

Theorem: If G is free abelian on X where $|X| = r$, then $G \cong \mathbb{Z}^r$.

Theorem: If $X = \{x_i\}_{i=1}^r$, then a basis for $\mathbb{Z}^r$ is given by

$$\{(1, 0, 0, \cdots), (0, 1, 0, \cdots), \cdots, (0, \cdots, 0, 1)\} \coloneqq \{e_1, e_2, \cdots, e_r\}$$

Proof: Use the map $\phi : G \to \mathbb{Z}^r$ where $x_i \mapsto e_i$, and check that this is an isomorphism of groups.

Theorem: Let G be free abelian with two bases X, X', then $|X| = |X|'$.

Definition: Let G be free abelian, then if X is a basis then $|X|$ is called the *rank* of of G.

8 Thursday September 5th

8.1 Rings

Recall the definition of a ring: A *ring* $(R, +, \times)$ is a set with binary operations such that

1. $(R, +)$ is a group,
2. $(R, \times)$ is a monoid.

Examples: $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, or the ring of $n \times n$ matrices, or $\mathbb{Z}_n$.

A ring is *commutative* iff $ab = ba$ for every $a, b \in R$, and *a ring with unity* is a ring such that $\exists 1 \in R$ such that $a1 = 1a = a$.

Exercise: Show that 1 is unique if it exists.

In a ring with unity, an element $a \in R$ is a *unit* iff $\exists b \in R$ such that $ab = ba = 1$.

Definition: A ring with unity is a **division ring** $\iff$ every nonzero element is a unit.

Definition: A division ring is a *field* $\iff$ it is commutative.

Definition: Suppose that $a, b \neq 0$ with $ab = 0$. Then a, b are said to be *zero divisors.*

Definition: A commutative ring without zero divisors is an *integral domain.*

Example: In $\mathbb{Z}_n$, an element a is a zero divisor iff $\gcd(a, n) \neq 1$.

Fact: In a ring with no zero divisors, we have

$$ab = ac \text{ and } a \neq 0 \implies b = c.$$

Theorem: Every field is an integral domain.

Proof: Let R be a field. If $ab = 0$ and $a \neq 0$, then a^{-1} exists and so $b = 0$.

■

Theorem: Any finite integral domain is a field.

Proof:

Idea: Similar to the pigeonhole principle.

Let $D = \{0, 1, a_1, \cdots, a_n\}$ be an integral domain. Let $a_j \neq 0, 1$ be arbitrary, and consider $a_j D = \left\{a_j x \;\middle|\; x \in D \setminus \{0\}\right\}$.

Then $a_j D = D \setminus \{0\}$ as sets. But

$$a_j D = \{a_j, a_j a_1, a_j a_2, \cdots, a_j a_n\}.$$

Since there are no zero divisors, 0 does not occur among these elements, so some $a_j a_k$ must be equal to 1.

■

8.2 Field Extensions

If $F \leq E$ are fields, then E is a vector space over F, for which the dimension turns out to be important.

Definition: We can consider

$$\mathrm{Aut}(E/F) \coloneqq \left\{\sigma : E \circlearrowleft \;\middle|\; f \in F \implies \sigma(f) = f\right\},$$

i.e. the field automorphisms of E that fix F.

Examples of field extensions: $\mathbb{C} \to \mathbb{R} \to \mathbb{Q}$.

Let $F(x)$ be the smallest field containing both F and x. Given this, we can form a diagram

$$
\begin{tikzcd}
 & F(x,y) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
F(x) \arrow[dr, dash] & {} \arrow[d, dash] & F(y) \arrow[dl, dash] \\
 & F &
\end{tikzcd}
$$

Let $F[x]$ the polynomials with coefficents in F.

Theorem: Let F be a field and $f(x) \in F[x]$ be a non-constant polynomial. Then there exists an $F \to E$ and some $\alpha \in E$ such that $f(\alpha) = 0$.

Proof: Since $F[x]$ is a unique factorization domain, given $f(x)$ we can find an irreducible $p(x)$ such that $f(x) = p(x)g(x)$ for some $g(x)$. So consider $E = F[x]/(p)$.

Since p is irreducible, (p) is a prime ideal, but in $F[x]$ prime ideals are maximal and so E is a field.

Then define

$$
\begin{aligned}
\psi : F &\to E \\
a &\mapsto a + (p).
\end{aligned}
$$

Then ψ is a homomorphism of rings: supposing $\psi(\alpha) = 0$, we must have $\alpha \in (p)$. But all such elements are multiples of a polynomial of degree $d \geq 1$, and α is a scalar, so this can only happen if $\alpha = 0$.

Then consider $\alpha = x + (p)$; the claim is that $p(\alpha) = 0$ and thus $f(\alpha) = 0$. We can compute

$$
\begin{aligned}
p(x + (p)) &= a_0 + a_1(x + (p)) + \cdots + a_n(x + (p))^n \\
&= p(x) + (p) = 0.
\end{aligned}
$$

■

Example: $\mathbb{R}[x]/(x^2+1)$ over $\mathbb{R}$ is isomorphic to $\mathbb{C}$ as a field.

8.3 Algebraic and Transcendental Elements

Definition: An element $\alpha \in E$ with $F \to E$ is **algebraic** over F iff there is a nonzero polynomial in $f \in F[x]$ such that $f(\alpha) = 0$.

Otherwise, α is said to be **transcendental**.

Examples:

- $\sqrt{2} \in \mathbb{R} \leftarrow \mathbb{Q}$ is algebraic, since it satisfies $x^2 - 2$.
- $\sqrt{-1} \in \mathbb{C} \leftarrow \mathbb{Q}$ is algebraic, since it satisfies $x^2 + 1$.
- $\pi, e \in \mathbb{R} \leftarrow \mathbb{Q}$ are transcendental

  > This takes some work to show.

An *algebraic number* $\alpha \in \mathbb{C}$ is an element that is algebraic over $\mathbb{Q}$.

Fact: The set of algebraic numbers forms a field.

Definition: Let $F \leq E$ be a field extension and $\alpha \in E$. Define a map

$$\begin{aligned}\phi_\alpha : F[x] &\to E \\ \phi_\alpha(f) &= f(\alpha).\end{aligned}$$

This is a homomorphism of rings and referred to as the *evaluation homomorphism.*

Theorem: Then ϕ_α is injective iff α is transcendental.

> Note: otherwise, this map will have a kernel, which will be generated by a single element that is referred to as the **minimal polynomial** of α.

8.4 Minimal Polynomials

Theorem: Let $F \leq E$ be a field extension and $\alpha \in E$ algebraic over F. Then

1. There exists a polynomial $p \in F[x]$ of minimal degree such that $p(\alpha) = 0$.
2. p is irreducible.
3. p is unique up to a constant.

Proof:

Since α is algebraic, $f(\alpha) = 0$. So write f in terms of its irreducible factors, so $f(x) = \prod p_j(x)$ with each p_j irreducible. Then $p_i(\alpha) = 0$ for some i because we are in a field and thus don't have zero divisors.

So there exists at least one $p_i(x)$ such that $p(\alpha) = 0$, so let q be one such polynomial of minimal degree.

Suppose that $\deg q < \deg p_i$. Using the Euclidean algorithm, we can write $p(x) = q(x)c(x) + r(x)$ for some c, and some r where $\deg r < \deg q$.

But then $0 = p(\alpha) = q(\alpha)c(\alpha) + r(\alpha)$, but if $q(\alpha) = 0$, then $r(\alpha) = 0$. So $r(x)$ is identically zero, and so $p(x) - q(x) = c(x) = c$, a constant.

$\blacksquare$

Definition: Let $\alpha \in E$ be algebraic over F, then the unique monic polynomial $p \in F[x]$ of minimal degree such that $p(\alpha) = 0$ is the **minimal polynomial** of α.

Example: $\sqrt{1+\sqrt{2}}$ has minimal polynomial $x^4 + x^2 - 1$, which can be found by raising it to the 2nd and 4th power and finding a linear combination that is constant.

9 Tuesday September 10th

9.1 Vector Spaces

Definition: Let $\mathbb{F}$ be a field. A **vector space** is an abelian group V with a map $\mathbb{F} \times V \to V$ such that

- $\alpha(\beta\mathbf{v}) = (\alpha\beta)\mathbf{v}$
- $(\alpha+\beta)\mathbf{v} = \alpha\mathbf{v} + \beta\mathbf{v}$,
- $\alpha(\mathbf{v}+\mathbf{w}) = \alpha\mathbf{v} + \alpha\mathbf{w}$
- $1\mathbf{v} = \mathbf{v}$

Examples: $\mathbb{R}^n, \mathbb{C}^n, F[x] = \mathrm{span}(\left\{1, x, x^2, \cdots\right\}), L^2(\mathbb{R})$

Definition: Let V be a vector space over $\mathbb{F}$; then a set $W \subseteq V$ *spans* V iff for every $\mathbf{v} \in V$, one can write $\mathbf{v} = \sum \alpha_i \mathbf{w}_i$ where $\alpha_i \in \mathbb{F},\ \mathbf{w}_i \in W$.

Definition: V is *finite dimensional* if there exists a finite spanning set.

Definition: A set $W \subseteq V$ is *linearly independent* iff

$$\sum \alpha_i \mathbf{w}_i = \mathbf{0} \implies \alpha_i = 0 \text{ for all } i.$$

Definition: A *basis* for V is a set $W \subseteq V$ such that

1. W is linearly independent, and
2. W spans V.

A basis is a midpoint between a spanning set and a linearly independent set.

We can add vectors to a set until it is spanning, and we can throw out vectors until the remaining set is linearly independent. This is encapsulated in the following theorems:

Theorem: If W spans V, then some subset of W spans V.

Theorem: If W is a set of linearly independent vectors, then some superset of W is a basis for V.

Fact: Any finite-dimensional vector spaces has a finite basis.

Theorem: If W is a linearly independent set and B is a basis, then $|B| \leq |W|$.

Corollary: Any two bases have the same number of elements.

> So we define the dimension of V to be the number of elements in any basis, which is a unique number.

9.2 Algebraic Extensions

Definition: $E \geq F$ is an algebraic extension iff every $\alpha \in E$ is algebraic of F.

Definition: $E \geq F$ is a *finite extension* iff E is finite-dimensional as an F-vector space.

Notation: $[E : F] = \dim_F E$, the dimension of E as an F-vector space.

Observation: If $E = F(\alpha)$ where α is algebraic over F, then E is an algebraic extension of F.

Observation: If $E \geq F$ and $[E : F] = 1$, then $E = F$.

Theorem: If $E \geq F$ is a finite extension, then E is algebraic over F.

Proof: Let $\beta \in E$. Then the set $\left\{1, \beta, \beta^2, \cdots\right\}$ is not linearly independent. So $\sum_{i=0}^{n} c_i \beta^i = 0$ for some n and some c_i. But then β is algebraic. ■

> Note that the converse is not true in general. *Example*: Let $E = \overline{\mathbb{R}}$ be the algebraic numbers. Then $E \geq \mathbb{Q}$ is algebraic, but $[E : \mathbb{Q}] = \infty$.

Theorem: Let $K \geq E \geq F$, then $[K : F] = [K : E][E : F]$.

Proof: Let $\{\alpha_i\}^m$ be a basis for E/F Let $\{\beta_i\}^n$ be a basis for K/E. Then the RHS is mn.

Claim: $\{\alpha_i \beta_j\}^{m,n}$ is a basis for K/F.

Linear independence:

$$\begin{aligned} \sum_{i,j} c_{ij} \alpha_i \beta_j &= 0 \\ \implies \sum_j \sum_i c_{ij} \alpha_i \beta_j &= 0 \\ \implies \sum_i c_{ij} \alpha_i &= 0 \quad \text{since } \beta \text{ form a basis} \\ \implies \sum c_{ij} &= 0 \quad \text{since } \alpha \text{ form a basis.} \end{aligned}$$

Exercise: Show this is also a spanning set.

■

Corollary: Let $E_r \geq E_{r-1} \geq \cdots \geq E_1 \geq F$, then

$$[E_r : F] = [E_r : E_{r-1}][E_{r-1} : E_{r-2}] \cdots [E_2 : E_1][E_1 : F].$$

Observation: If $\alpha \in E \geq F$ and α is algebraic over F where $E \geq F(\alpha) \geq F$, then $F(\alpha)$ is algebraic (since $[F(\alpha) : F] < \infty$) and $[F(\alpha) : F]$ is the degree of the minimal polynomial of α over F.

Corollary: Let $E = F(\alpha) \geq F$ where α is algebraic. Then

$$\beta \in F(\alpha) \implies \deg \min(\beta, F) \,\Big|\, \deg \min(\alpha, F).$$

Proof: Since $F(\alpha) \geq F(\beta) \geq F$, we have $[F(\alpha) : F] = [F(\alpha) : F(\beta)][F(\beta) : F]$. But just note that

$$\begin{aligned} [F(\alpha) : F] &= \deg \min(\alpha, F) \text{ and} \\ [F(\beta) : F] &= \deg \min(\beta, F). \end{aligned}$$

■

Theorem: Let $E \geq F$ be algebraic, then

$$[E : F] < \infty \iff E = F(\alpha_1, \cdots, \alpha_n) \text{ for some } \alpha_n \in E.$$

9.3 Algebraic Closures

Definition: Let $E \geq F$, and define

$$\overline{F_E} = \left\{ \alpha \in E \,\middle|\, \alpha \text{ is algebraic over } F \right\}$$

to be the **algebraic closure of F in E**.

Example: $\mathbb{Q} \hookrightarrow \mathbb{C}$, while $\overline{\mathbb{Q}} = \mathbb{A}$ is the field of algebraic numbers, which is a dense subfield of $\mathbb{C}$.

Proposition: $\overline{F_E}$ is a always field.

Proof: Let $\alpha, \beta \in \overline{F_E}$, so $[F(\alpha, \beta) : F] < \infty$. Then $F(\alpha, \beta) \subseteq \overline{F_E}$ is algebraic over F and

$$\alpha \pm \beta, \quad \alpha\beta, \quad \frac{\alpha}{\beta} \quad \in F(\alpha, \beta).$$

So $\overline{F_E}$ is a subfield of E and thus a field.

Definition: A field F is **algebraically closed** iff every non-constant polynomial in $F[x]$ is a root in F. Equivalently, every polynomial in $F[x]$ can be factored into linear factors.

If F is algebraically closed and $E \geq F$ and E is algebraic, then $E = F$.

9.3.1 The Fundamental Theorem of Algebra

Theorem (Fundamental Theorem of Algebra): $\mathbb{C}$ is an algebraically closed field.

Proof:

Liouville's theorem: A bounded entire function $f : \mathbb{C} \circlearrowleft$ is constant.

- *Bounded* means $\exists M \,\Big|\, z \in \mathbb{C} \implies |f(z)| \leq M$.
- *Entire* means analytic everywhere.

Let $f(z) \in \mathbb{C}[z]$ be a polynomial without a zero which is non-constant.

Then $\dfrac{1}{f(z)} : \mathbb{C} \circlearrowleft$ is analytic and bounded, and thus constant, and contradiction.

■

9.4 Geometric Constructions:

Given the tools of a straightedge and compass, what real numbers can be constructed? Let $\mathcal{C}$ be the set of such numbers.

Theorem: C is a subfield of $\mathbb{R}$.

10 Thursday September 12th

10.1 Geometric Constructions

Definition: A real number α is said to be **constructible** iff $|\alpha|$ is constructible using a ruler and compass. Let $\mathcal{C}$ be the set of constructible numbers.

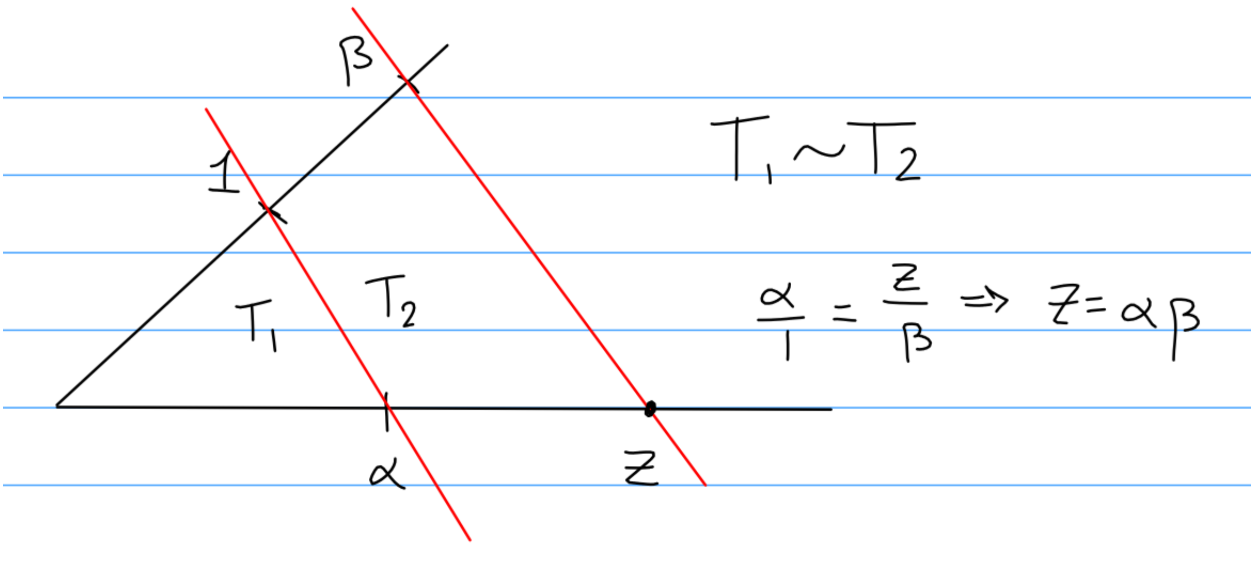
Note that ± 1 is constructible, and thus so is $\mathbb{Z}$.

Theorem: $\mathcal{C}$ is a field.

Proof: It suffices to construct $\alpha \pm \beta,\ \alpha\beta,\ \alpha/\beta$.

Showing $\pm$ and inverses: Relatively easy.

Showing closure under products:



Corollary: $\mathbb{Q} \leq \mathcal{C}$ is a subfield.

Can we get all of $\mathbb{R}$ with $\mathcal{C}$? The operations we have are

1. Intersect 2 lines (gives nothing new)
2. Intersect a line and a circle
3. Intersect 2 circles

Operation (3) reduces to (2) by subtracting two equations of a circle ($x^2 + y^2 + ax + by + c$) to get an equation of a line.

Operation (2) reduces to solving quadratic equations.

Theorem: $\mathcal{C}$ contains precisely the real numbers obtained by adjoining finitely many square roots of elements in $\mathbb{Q}$.

Proof: Need to show that $\alpha \in \mathcal{C} \implies \sqrt{\alpha} \in \mathcal{C}$.

- Bisect PA to get B.
- Draw a circle centered at B.
- Let Q be intersection of circle with y axis and O be the origin.
- Note triangles 1 and 2 are similar, so

$$\frac{OQ}{OA} = \frac{PO}{OQ} \implies (OQ)^2 = (PO)(OA) = 1\alpha.$$

$\blacksquare$

Corollary: Let $\gamma \in \mathcal{C}$ be constructible. Then there exist $\{\alpha_i\}_{i=1}^n$ such that

$$\gamma = \prod_{i=1}^{n} \alpha_i \quad \text{and} \quad [\mathbb{Q}(\alpha_1, \cdots, \alpha_j) : \mathbb{Q}(\alpha_1, \cdots, \alpha_{j-1})] = 2,$$

and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^d$ for some d.

Applications:

Doubling the cube: Given a cube of size 1, can we construct one of size 2? To do this, we'd need $x^3 = 2$. But note that $\min(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2 = f(x)$ is irreducible over $\mathbb{Q}$. So $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 2^d$ for any d, so this can not be constructible.

Trisections of angles: We want to construct regular polygons, so we'll need to construct angles. We can get some by bisecting known angles, but can we get all of them?

Example: Attempt to construct 20° by trisecting the known angle 60°, which is constructible using a triangle of side lengths $1, 2, \sqrt{3}$.

If 20° were constructible, $\cos 20^\circ$ would be as well. There is an identity

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

Letting $\theta = 20^\circ$ so $3\theta = 60^\circ$, we obtain

$$\frac{1}{2} = 4(\cos 20^\circ)^3 - 3\cos 20^\circ,$$

so if we let $x = \cos 20^\circ$ then x satisfies the polynomial $f(x) = 8x^3 - 6x - 1$, which is irreducible. But then $[\mathbb{Q}(20^\circ) : \mathbb{Q}] = 3 \neq 2^d$, so $\cos 20^\circ \notin \mathcal{C}$.

10.2 Finite Fields

Definition: The *characteristic* of F is the smallest $n \geq 0$ such that $n1 = 0$, or 0 if such an n does not exist.

Exercise: For a field F, show that char $F = 0$ or p a prime.

Note that if char $F = 0$, then $\mathbb{Z} \in F$ since $1,\ 1+1,\ 1+1+1, \cdots$ are all in F. Since inverses must also exist in F, we must have $\mathbb{Q} \in F$ as well. So char $F = 0 \iff F$ is infinite.

If char $F = p$, it follows that $\mathbb{Z}_p \subset F$.

Theorem:

$$\text{For } E \geq F \text{ where } [E:F] = n \text{ and } F \text{ finite },\quad |F| = q \implies |E| = q^n.$$

Proof: E is a vector space over F. Let $\{v_i\}^n$ be a basis. Then $\alpha \in E \implies \alpha = \sum_{i=1}^{n} a_i v_i$ where each $a_i \in F$. There are q choices for each a_i, and n coefficients, yielding q^n distinct elements.

■

Corollary: Let E be a finite field where char $E = p$. Then $|E| = p^n$ for some n.

Theorem: Let $\mathbb{Z}_p \leq E$ with $|E| = p^n$. If $\alpha \in E$, then α satisfies

$$x^{p^n} - x \in \mathbb{Z}_p[x].$$

Proof: If $\alpha = 0$, we're done. So suppose $\alpha \neq 0$, then $\alpha \in E^\times$, which is a group of order $p^n - 1$. So $\alpha^{p^n-1} = 1$, and thus $\alpha\alpha^{p^n-1} = \alpha 1 \implies \alpha^{p^n} = \alpha$.

■

Definition: $\alpha \in F$ is an *nth root of unity* iff $\alpha^n = 1$. It is a *primitive* root of unity of n iff $k \leq n \implies \alpha^k \neq 1$ (so n is the smallest power for which this holds).

Fact: If F is a finite field, then $F^\times$ is a cyclic group.

Corollary: If $E \geq F$ with $[E:F] = n$, then $E = F(\alpha)$ for just a single element α.

Proof: Choose $\alpha \in E^\times$ such that $\langle \alpha \rangle = E^\times$. Then $E = F(\alpha)$.

■

Next time: Showing the existence of a field with p^n elements.

For now: derivatives.

Let $f(x) \in F[x]$ by a polynomial with a multiple zero $\alpha \in E$ for some $E \geq F$.

If it has multiplicity $m \geq 2$, then note that

$$f(x) = (x-\alpha)^m g(x) \implies f'(x)m(x-\alpha)^{m-1}g(x) + g'(x)(x-\alpha)^m \implies f'(\alpha) = 0.$$

So

$$\alpha \text{ a multiple zero of } f \implies f'(\alpha) = 0.$$

The converse is also useful.

Application: Let $f(x) = x^{p^n} - x$, then $f'(x) = p^n x^{p^n-1} - 1 = -1 \neq 0$, so all of the roots are distinct.

11 Tuesday September 17th

11.1 Finite Fields and Roots of Polynomials

Recall from last time:

Let $\mathbb{F}$ be a finite field. Then $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$ is *cyclic* (this requires some proof).

Let $f \in \mathbb{F}[x]$ with $f(\alpha) = 0$. Then α is a *multiple root* if $f'(\alpha) = 0$.

Lemma: Let $\mathbb{F}$ be a finite field with characteristic $p > 0$. Then

$$f(x) = x^{p^n} - x \in \mathbb{F}[x]$$

has p^n distinct roots.

Proof:

$$f'(x) = p^n x^{p^n-1} - 1 = -1,$$

since we are in char p.

This is identically -1, so $f'(x) \neq 0$ for any x. So there are no multiple roots. Since there are at most p^n roots, this gives exactly p^n distinct roots.

$\blacksquare$

Theorem: A field with p^n elements exists (denoted $\mathbb{GF}(p^n)$) for every prime p and every $n > 0$.

Proof: Consider $\mathbb{Z}_p \subseteq K \subseteq \overline{\mathbb{Z}}_p$ where K is the set of zeros of $x^{p^n} - x$. Then we claim K is a field.

Suppose $\alpha, \beta \in K$. Then $(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n}$.

We also have

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} - \alpha\beta \text{ and } \alpha^{-p^n} = \alpha^{-1}.$$

So K is a field and $|K| = p^n$.

$\blacksquare$

Corollary: Let F be a finite field. If $n \in \mathbb{N}^+$, then there exists an $f(x) \in F[x]$ that is irreducible of degree n.

Proof: Let F be a finite field, so $|F| = p^r$. By the previous lemma, there exists a K such that $\mathbb{Z}_p \subseteq k \subseteq \overline{F}$.

K is defined as

$$K := \left\{ \alpha \in F \;\middle|\; \alpha^{p^n} - \alpha = 0 \right\}.$$

We also have

$$F = \left\{ \alpha \in \overline{F} \;\middle|\; \alpha^{p^n} - \alpha = 0 \right\}.$$

Moreover, $p^{rs} = p^r p^{r(s-1)}$. So let $\alpha \in F$, then $\alpha^{p^r} - \alpha = 0$.

Then

$$\alpha^{p^{rn}} = \alpha^{p^r p^{r(n-1)}} = (\alpha^{p^r})^{p^{r(n-1)}} = \alpha^{p^{r(n-1)}},$$

and we can continue reducing this way to show that this is yields to $\alpha^{p^r} = \alpha$.

So $\alpha \in K$, and thus $F \leq K$. We have $[K : F] = n$ by counting elements. Now K is simple, because $K^\times$ is cyclic. Let β be the generator, then $K = F(\beta)$. This the minimal polynomial of β in F has degree n, so take this to be the desired $f(x)$.

■

11.2 Simple Extensions

Let $F \leq E$ and

$$\begin{aligned} \phi_\alpha : F[x] &\to E \\ f &\mapsto f(\alpha). \end{aligned}$$

denote the evaluation map.

Case 1: Suppose α is **algebraic** over F.

There is a kernel for this map, and since $F[x]$ is a PID, this ideal is generated by a single element – namely, the minimal polynomial of α.

Thus (applying the first isomorphism theorem), we have $F(\alpha) \supseteq E$ isomorphic to $F[x]/\min(\alpha, F)$. Moreover, $F(\alpha)$ is the smallest subfield of E containing F and α.

Case 2: Suppose α is **transcendental** over F.

Then $\ker \phi_\alpha = 0$, so $F[x] \hookrightarrow E$. Thus $F[x] \cong F[\alpha]$.

Definition: $E \geq F$ is a *simple extension* if $E = F(\alpha)$ for some $\alpha \in E$.

Theorem: Let $E = F(\alpha)$ be a simple extension of F where α is algebraic over F.

Then every $\beta \in E$ can be uniquely expressed as

$$\beta = \sum_{i=0}^{n-1} c_i \alpha^i \text{ where } n = \deg \min(\alpha, F).$$

Proof:

Existence: We have

$$F(\alpha) = \left\{ \sum_{i=1}^{r} \beta_i \alpha^i \;\middle|\; \beta_i \in F \right\},$$

so all elements look like polynomials in α.

Using the minimal polynomial, we can reduce the degree of any such element by rewriting α^n in terms of lower degree terms:

$$\begin{aligned} f(x) = \sum_{i=0}^{n} a_i x^i, \quad f(\alpha) = 0 \\ \implies \sum_{i=0}^{n} a_i \alpha^i = 0 \\ \implies \alpha^n = -\sum_{i=0}^{n-1} a_i \alpha^i. \end{aligned}$$

Uniqueness: Suppose $\sum c_i \alpha^i = \sum^{n-1} d_i \alpha^i$. Then $\sum^{n-1} (c_i - d_i)\alpha^i = 0$. But by minimality of the minimal polynomial, this forces $c_i - d_i = 0$ for all i.

■

Note: if α is algebraic over F, then $\left\{1, \alpha, \cdots \alpha^{n-1}\right\}$ is a basis for $F(\alpha)$ over F where $n = \deg \min(\alpha, F)$. Moreover,

$$[F(\alpha) : F] = \dim_F F(\alpha) = \deg \min(\alpha, F).$$

Note: adjoining any root of a minimal polynomial will yield isomorphic (usually not *identical*) fields. These are distinguished as subfields of the algebraic closure of the base field.

Theorem: Let $F \leq E$ with $\alpha \in E$ algebraic over F.

If $\deg \min(\alpha, F) = n$, then $F(\alpha)$ has dimension n over F, and $\left\{1, \alpha, \cdots, \alpha^{n-1}\right\}$ is a basis for $F(\alpha)$ over F.

Moreover, any $\beta \in F(\alpha)$, is *also* algebraic over F,and $\deg \min(\beta, F) \mid \deg \min(\alpha, F)$.

Proof of first part: Exercise.

Proof of second part: We want to show that β is algebraic over F.

We have

$$[F(\alpha) : F] = [F(\alpha) : F(\beta)][F(\beta) : F],$$

so $[F(\beta) : F]$ is less than n since this is a finite extension, and the division of degrees falls out immediately.

■

11.3 Automorphisms and Galois Theory

Let F be a field and $\overline{F}$ be its algebraic closure. Consider subfields of the algebraic closure, i.e. E such that $F \leq E \leq \overline{F}$. Then $E \geq F$ is an algebraic extension.

Definition: $\alpha, \beta \in E$ are *conjugates* iff $\min(\alpha, F) = \min(\beta, F)$.

Examples:

- $\sqrt[3]{3}$, $\sqrt[3]{3}\zeta$, $\sqrt[3]{3}\zeta^2$ are all conjugates, where $\zeta = e^{2\pi i/3}$.
- $\alpha = a + bi \in \mathbb{C}$ has conjugate $\bar{\alpha} = a - bi$, and

$$\min(\alpha, \mathbb{R}) = \min(\bar{\alpha}, \mathbb{R}) = x^2 - 2ax + (a^2 + b^2).$$

12 Thursday September 19th

12.1 Conjugates

Let $E \geq F$ be a field extension. Then $\alpha, \beta \in E$ are *conjugate* $\iff$ $\min(\alpha, F) = \min(\beta, F)$ in $F[x]$.

Example: $a + bi, a - bi$ are conjugate in $\mathbb{C}/\mathbb{R}$, since they both have minimal polynomial $x^2 - 2ax + (a^2 + b^2)$ over $\mathbb{R}$.

Theorem: Let F be a field and $\alpha, \beta \in E \geq F$ with $\deg \min(\alpha, F) = \deg \min(\beta, F)$, i.e.

$$[F(\alpha) : F] = [F(\beta) : F].$$

Then α, β are conjugates $\iff$ $F(\alpha) \cong F(\beta)$ under the map

$$\begin{aligned} \phi : F(\alpha) &\to F(\beta) \\ \sum_i a_i \alpha^i &\mapsto \sum_i a_i \beta^i. \end{aligned}$$

Proof: Suppose ϕ is an isomorphism.

Let

$$f := \min(\alpha, F) = \sum c_i x^i \text{ where } c_i \in F,$$

so $f(\alpha) = 0$.

Then

$$0 = f(\alpha) = f(\sum c_i \alpha^i) = \sum c_i \beta^i,$$

so β satisfies f as well, and thus $f = \min(\alpha, F) \mid \min(\beta, F)$.

But we can repeat this argument with f^{-1} and $g(x) := \min(\beta, F)$, and so we get an equality. Thus α, β are conjugates.

Conversely, suppose α, β are conjugates so that $f = g$. Check that ϕ is a homomorphism of fields, so that

$$\phi(x + y) = \phi(x) + \phi(y) \text{ and } \phi(xy) = \phi(x)\phi(y).$$

Then ϕ is clearly surjective, so it remains to check injectivity.

To see that ϕ is injective, suppose $f(z) = 0$. Then $\sum a_i \beta^i = 0$. But by linear independence, this forces $a_i = 0$ for all i, which forces $z = 0$. ■

Corollary: Let $\alpha \in \overline{F}$ be algebraic over F.

Then

1. $\phi : F(\alpha) \hookrightarrow \overline{F}$ for which $\phi(f) = f$ for all $f \in F$ maps α to one of its conjugates.
2. If $\beta \in \overline{F}$ is a conjugate of α, then there exists one isomorphism $\psi : F(\alpha) \to F(\beta)$ such that $\psi(f) = f$ for all $f \in F$.

Corollary: Let $f \in \mathbb{R}[x]$ and suppose $f(a + bi) = 0$. Then $f(a - bi) = 0$ as well.

Proof: We know $i, -i$ are conjugates since they both have minimal polynomial $f(x) = x^2 + 1$. By (2), we have an isomorphism $\mathbb{R}[i] \xrightarrow{\psi} \mathbb{R}[-i]$. We have $\psi(a + bi) = a - bi$, and $f(a + bi) = 0$.

This isomorphism commutes with f, so we in fact have

$$0 = \psi(f(a + bi)) = f(\psi(a - bi)) = f(a - bi).$$

■

12.2 Fixed Fields and Automorphisms

Definition: Let F be a field and $\psi : F\circlearrowleft$ is an *automorphism* iff ψ is an isomorphism.

Definition: Let $\sigma : E\circlearrowleft$ be an automorphism. Then σ is said to *fix* $a \in E$ iff $\sigma(a) = a$. For any subset $F \subseteq E$, σ fixes F iff σ fixes every element of F.

Example: Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{5}) \supseteq \mathbb{Q} = F$.

A basis for E/F is given by $\left\{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\right\}$. Suppose $\psi : E\circlearrowleft$ fixes $\mathbb{Q}$. By the previous theorem, we must have $\psi(\sqrt{2}) = \pm\sqrt{2}$ and $\psi(\sqrt{5}) = \pm\sqrt{5}$.

What is fixed by ψ? Suppose we define ψ on generators, $\psi(\sqrt{2}) = -\sqrt{2}$ and $\psi(\sqrt{5}) = \sqrt{5}$.

Then

$$f(c_0 + c_1\sqrt{2} + c_2\sqrt{5} + c_3\sqrt{10}) = c_0 - c_1\sqrt{2} + c_2\sqrt{5} - c_3\sqrt{10}.$$

This forces $c_1 = 0, c_3 = 0$, and so ψ fixes $\left\{c_0 + c_2\sqrt{5}\right\} = \mathbb{Q}(\sqrt{5})$.

Theorem: Let I be a set of automorphisms of E and define

$$E_I = \left\{\alpha \in E \;\middle|\; \sigma(a) = a \ \forall \sigma \in I\right\}$$

Then $E_I \leq E$ is a subfield.

Proof: Let $a, b \in E_i$. We need to show $a \pm b, ab, b \neq 0 \implies b^{-1} \in I$.

We have $\sigma(a \pm b) = \sigma(a) \pm \sigma(b) = a + b \in I$ since σ fixes everything in I. Moreover

$$\sigma(ab) = \sigma(a)\sigma(b) = ab \in I \quad \text{and} \quad \sigma(b^{-1}) = \sigma(b)^{-1} = b^{-1} \in I.$$

■

Definition: Given a set I of automorphisms of F, E_I is called the *fixed field* of E under I.

Theorem: Let E be a field and $A = \left\{ \sigma : E \circlearrowleft \;\middle|\; \sigma \text{ is an automorphism} \right\}$. Then A is a group under function composition.

Theorem: Let E/F be a field extension, and define

$$G(E/F) = \left\{ \sigma : E \circlearrowleft \;\middle|\; f \in F \implies \sigma(f) = f \right\}.$$

Then $G(E/F) \leq A$ is a subgroup which contains F.

Proof: This contains the identity function.

Now if $\sigma(f) = f$ then $f = \sigma^{-1}(f)$, and

$$\sigma, \tau \in G(E/F) \implies (\sigma \circ \tau)(f) = \sigma(\tau(f)) = \sigma(f) = f.$$

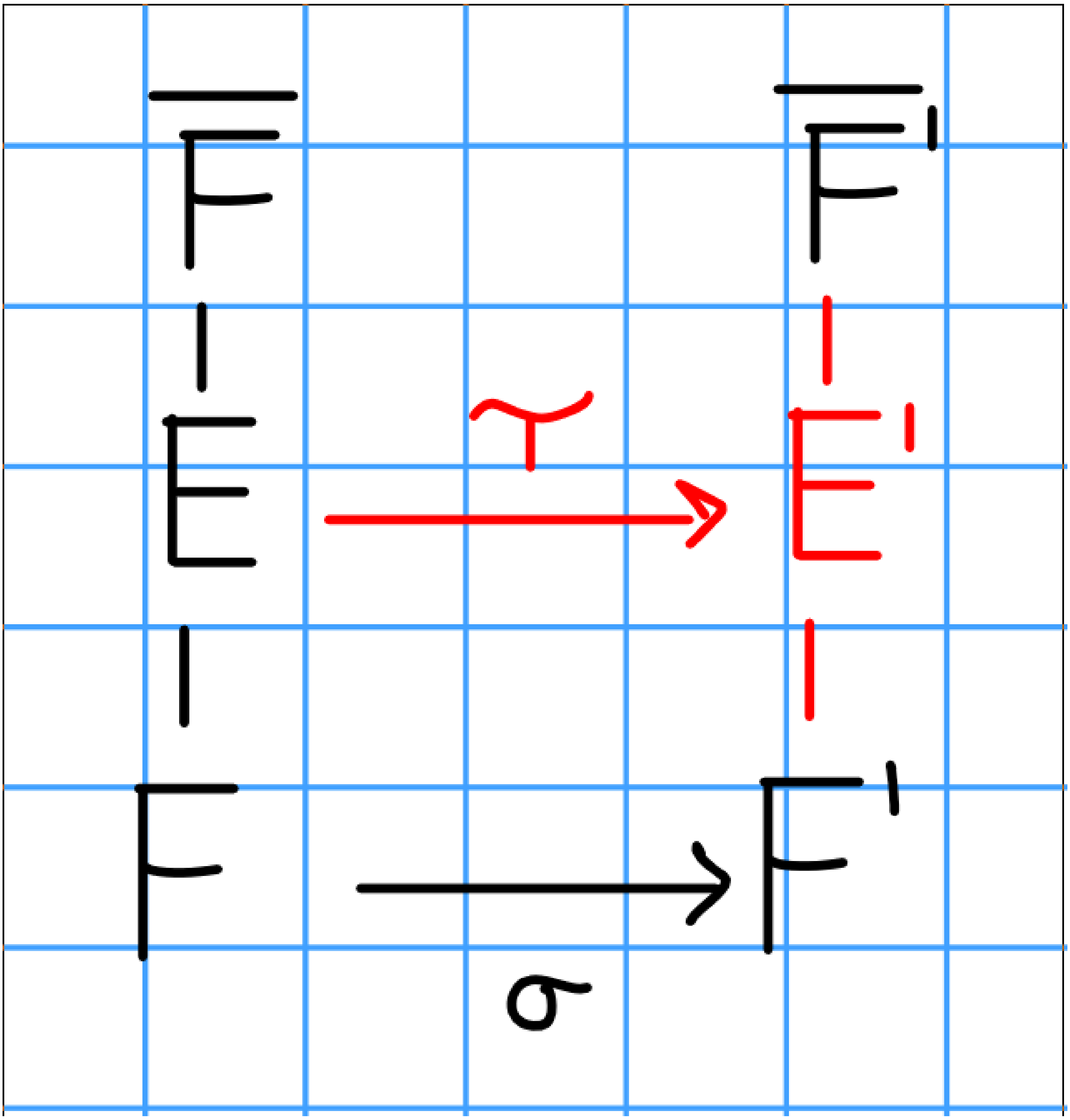
■

Note $G(E/F)$ is called the group of automorphisms of E fixing F, i.e. **the Galois Group.**

Theorem (Isomorphism Extension): Suppose $F \leq E \leq \overline{F}$, so E is an algebraic extension of F.

Suppose similarly that we have $F' \leq E' \leq \overline{F}'$, where we want to find E'.

Then any $\sigma : F \to F'$ that is an isomorphism can be lifted to some $\tau : E \to E'$, where $\tau(f) = \sigma(f)$ for all $f \in F$.



13 Tuesday October 1st

13.1 Isomorphism Extension Theorem

Suppose we have $F \leq E \leq \overline{F}$ and $F' \leq E' \leq \overline{F}'$. Supposing also that we have an isomorphism $\sigma : F \to F'$, we want to extend this to an isomorphism from E to *some* subfield of $\overline{F}'$ over F'.

Theorem: Let E be an algebraic extension of F and $\sigma : F \to F'$ be an isomorphism of fields. Let $\overline{F}'$ be the algebraic closure of F'.

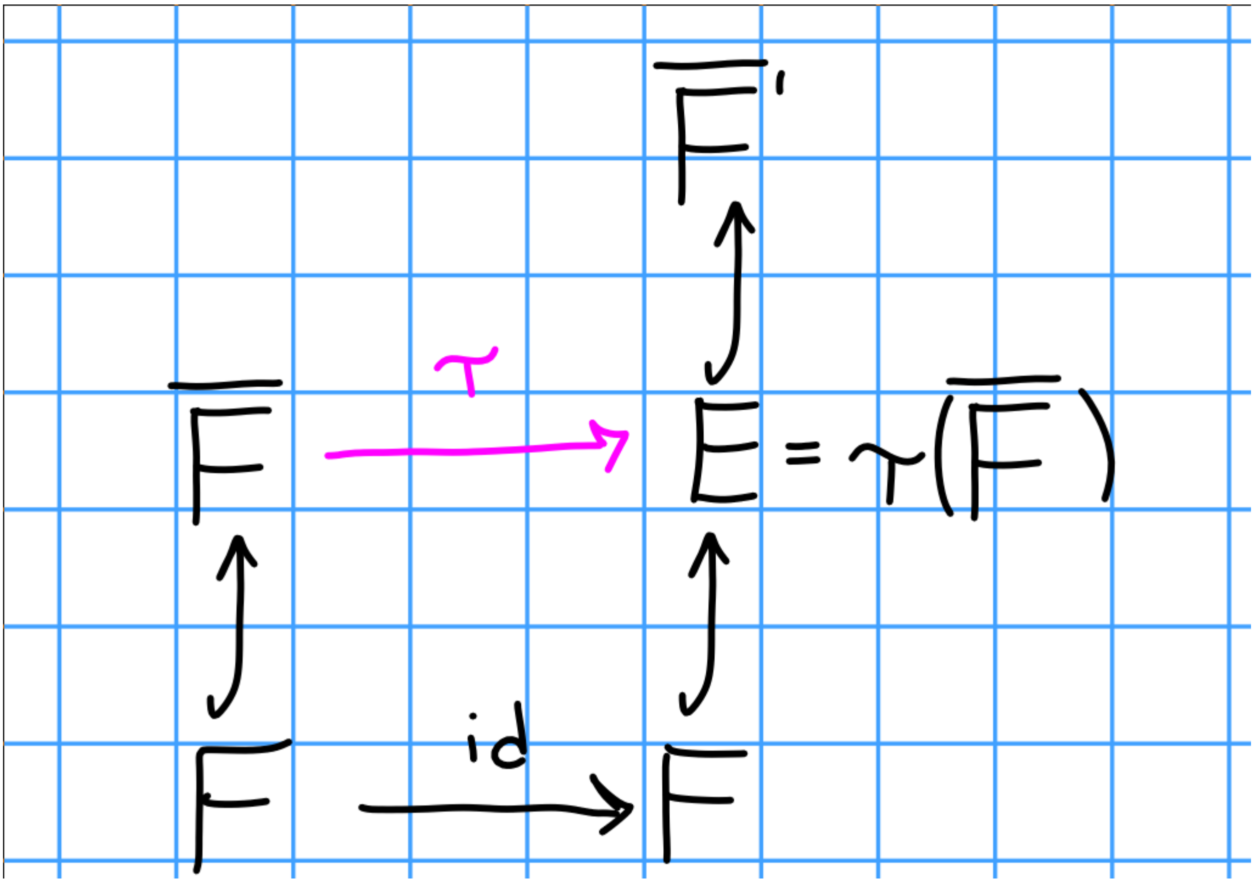
Then there exists a $\tau : E \to E'$ where $E' \leq F'$ such that $\tau(f) = \sigma(f)$ for all $f \in F$.

Proof: See Fraleigh. Uses Zorn's lemma.

■

Corollary: Let F be a field and $\overline{F}, \overline{F}'$ be algebraic closures of F. Then $\overline{F} \cong \overline{F}'$.

Proof: Take the identity $F \to F$ and lift it to some $\tau : \overline{F} \to E = \tau(\overline{F})$ inside $\overline{F}'$.



Then $\tau(\overline{F})$ is algebraically closed, and $\overline{F}' \geq \tau(\overline{F})$ is an algebraic extension. But then $\overline{F}' = \tau(\overline{F})$. ■

Corollary: Let $E \geq F$ be an algebraic extension with $\alpha, \beta \in E$ conjugates. Then the conjugation isomorphism that sends $\alpha \to \beta$ can be extended to E.

Proof:

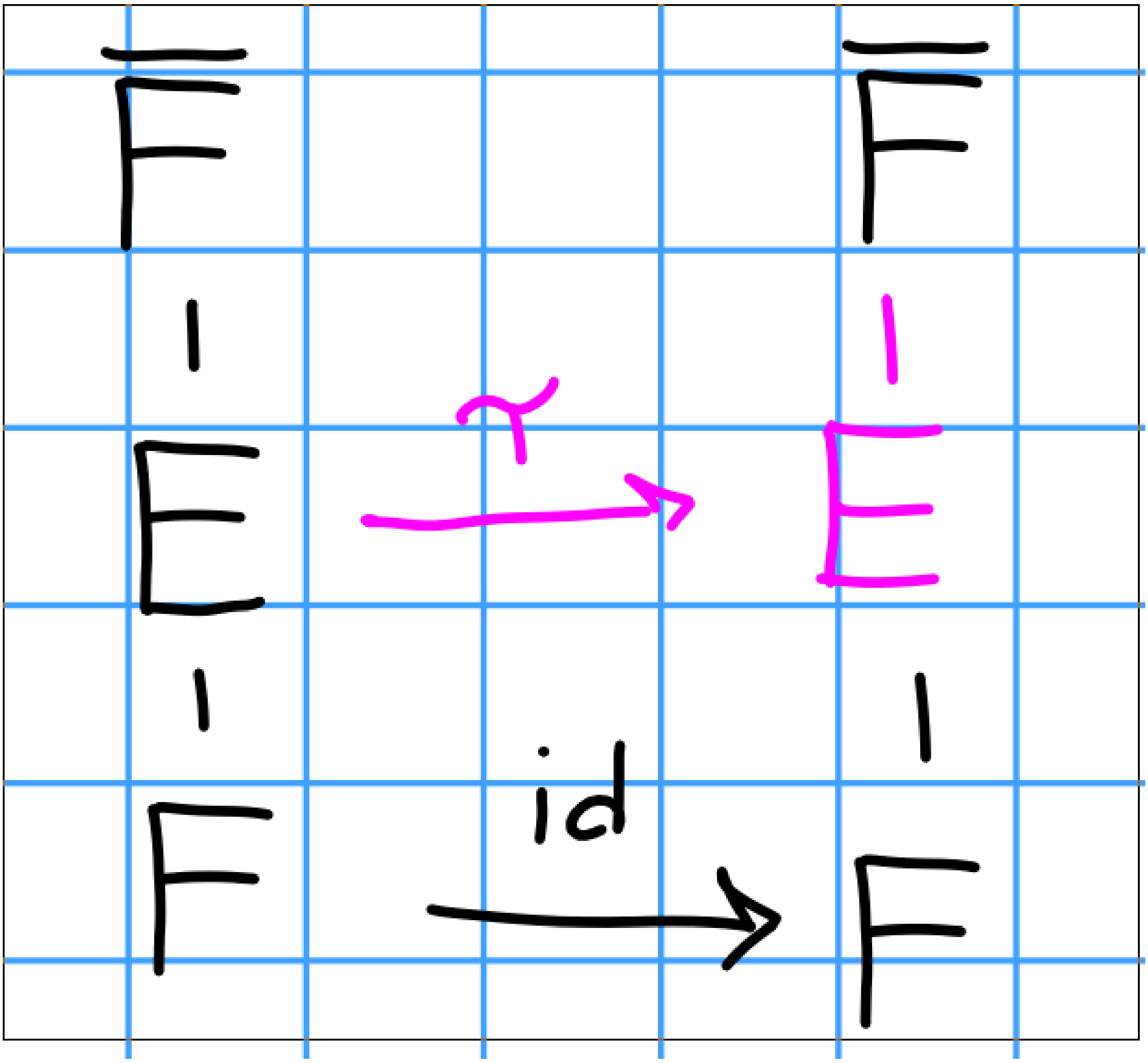
$$
\begin{tikzcd}
\overline{F} \arrow[d, dash] & \overline{F} \arrow[d, dash] \\
E \arrow[r, "\tau"] \arrow[d, dash] & E \arrow[d, dash] \\
F(\alpha) \arrow[r, "\psi"] \arrow[d, dash] & F(\beta) \arrow[d, dash] \\
F \arrow[r, "id"] & F
\end{tikzcd}
$$

> Note: Any isomorphism needs to send algebraic elements to algebraic elements, and even more strictly, conjugates to conjugates.

Counting the number of isomorphisms:

Let $E \geq F$ be a finite extension. We want to count the number of isomorphisms from E to a subfield of $\overline{F}$ that leave F fixed.

I.e., how many ways can we fill in the following diagram?



Let $G(E/F) \coloneqq \mathrm{Gal}(E/F)$; this will be a finite group if $[E : F] < \infty$.

Theorem: Let $E \geq F$ with $[E : F] < \infty$ and $\sigma : F \to F'$ be an isomorphism.

Then the number of isomorphisms $\tau : E \to E'$ extending σ is *finite*.

Proof: Since $[E : F]$ is finite, we have $F_0 \coloneqq F(\alpha_1, \alpha_2, \cdots, \alpha_t)$ for some $t \in \mathbb{N}$. Let $\tau : F_0 \to E'$ be an isomorphism extending σ.

Then $\tau(\alpha_i)$ must be a conjugate of α_i, of which there are only finitely many since $\deg \min(\alpha_j, F)$ is finite. So there are at most $\prod_i \deg \min(\alpha_i, F)$ isomorphisms.

Example: $f(x) = x^3 - 2$, which has roots $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta$, $\sqrt[3]{\zeta}^2$.

Two other concepts to address:

- Separability (multiple roots)
- Splitting Fields (containing all roots)

Definition: Let

$$\{E : F\} \coloneqq \left| \left\{ \sigma : E \to E' \;\middle|\; \sigma \text{ is an isomorphism extending id} : F \to F \right\} \right|,$$

and define this to be the *index*.

Theorem: Suppose $F \leq E \leq K$, then

$$\{K : F\} = \{K : E\} \{E : F\} .$$

Proof: Exercise.

■

Example: $\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}$, which is an extension of *degree* 4. It also turns out that $\left\{ \mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q} \right\} = 4$ as well.

Questions:

1. When does $[E : F] = \{E : F\}$? (This is always true in characteristic zero.)
2. When is $\{E : F\} = |\mathrm{Gal}(E/F)|$?

Note that in this example, $\sqrt{5} \mapsto \pm\sqrt{5}$ and likewise for $\sqrt{2}$, so any isomorphism extending the identity must in fact be an *automorphism*.

We have automorphisms

$$\begin{aligned}
\sigma_1 &: (\sqrt{2}, \sqrt{5}) \mapsto (-\sqrt{2}, \sqrt{5}) \\
\sigma_2 &: (\sqrt{2}, \sqrt{5}) \mapsto (\sqrt{2}, -\sqrt{5}),
\end{aligned}$$

as well as id and $\sigma_1 \circ \sigma_2$. Thus $\mathrm{Gal}(E/F) \cong \mathbb{Z}_2^2$.

13.2 Separable Extensions

Goal: When is $\{E : F\} = [E : F]$? We'll first see what happens for simple extensions.

Definition: Let $f \in F[x]$ and α be a zero of f in $\overline{F}$.

The maximum ν such that $(x - \alpha)^\nu \;\Big|\; f$ is called the *multiplicity* of f.

Theorem: Let f be irreducible.

Then all zeros of f in $\overline{F}$ have the same multiplicity.

Proof: Let α, β satisfy f, where f is irreducible. Then consider the following lift:

$$
\begin{tikzcd}
\overline{F} & & & & \overline{F} \\
F(\alpha) \arrow[u, dash] \arrow[rrrr, "\sim\psi"] & & & & F(\beta) \arrow[u, dash] \\
F \arrow[u, dash] \arrow[rrrr, "\mathrm{id}"] & & & & F \arrow[u, dash]
\end{tikzcd}
$$

This induces a map

$$
\begin{aligned}
F(\alpha)[x] &\xrightarrow{\tau} F(\beta)[x] \\
\sum c_i x^i &\mapsto \sum \psi(c_i) x^i,
\end{aligned}
$$

so $x \mapsto x$ and $\alpha \mapsto \beta$, so $x \mapsto x$ and $\alpha \mapsto \beta$.

Then $\tau(f(x)) = f(x)$ and

$$\tau((x-\alpha)^\nu) = (x-\beta)^\nu.$$

So write $f(x) = (x-\alpha)^\nu h(x)$, then

$$\tau(f(x)) = \tau((x-\alpha)^\nu)\tau(h(x)).$$

Since $\tau(f(x)) = f(x)$, we then have

$$f(x) = (x - \beta)^{\nu} \tau(h(x)).$$

So we get $\text{mult}(\alpha) \leq \text{mult}(\beta)$. But repeating the argument with α, β switched yields the reverse inequality, so they are equal.

■

Observation: If $F(\alpha) \to E'$ extends the identity on F, then $E' = F(\beta)$ where β is a root of $f := \min(\alpha, F)$. Thus we have

$$\{F(\alpha) : F\} = |\{\text{distinct roots of } f\}|.$$

Moreover,

$$[F(\alpha) : F] = \{F(\alpha) : F\} \, \nu$$

where ν is the multiplicity of a root of $\min(\alpha, F)$.

Theorem: Let $E \geq F$, then $\{E : F\} \mathrel{\Big|} [E : F]$.

14 Thursday October 3rd

When can we guarantee that there is a $\tau : E \circlearrowleft$ lifting the identity?

If E is *separable*, then we have $|\text{Gal}(E/F)| = \{E : F\} \, [E : F]$.

Fact: $\{F(\alpha) : F\}$ is equal to number of *distinct* zeros of $\min(\alpha, F)$.

If F is algebraic, then $[F(\alpha) : F]$ is the degree of the extension, and $\{F(\alpha) : F\} \mathrel{\Big|} [F(\alpha) : F]$.

Theorem: Let $E \geq F$ be finite, then $\{E : F\} \mathrel{\Big|} [E : F]$.

Proof: If $E \geq F$ is finite, $E = F(\alpha_1, \cdots, \alpha_n)$.

So $\min(\alpha_i, F)$ has a_j as a root, so let n_j be the number of distinct roots, and v_j the respective multiplicities.

Then

$$[F : F(\alpha_1, \cdots, \alpha_{n-1})] = n_j v_j = v_j \{F : F(\alpha_1, \cdots, \alpha_{n-1})\}.$$

So $[E : F] = \prod_j n_j v_j$ and $\{E : F\} = \prod_j n_j$, and we obtain divisibility.

■

Definitions:

1. An extension $E \geq F$ is **separable** iff $[E : F] = \{E : F\}$
2. An element $\alpha \in E$ is **separable** iff $F(\alpha) \geq F$ is a separable extension.

3. A polynomial $f(x) \in F[x]$ is **separable** iff $f(\alpha) = 0 \implies \alpha$ is separable over F.

Lemma:

1. α is separable over F iff $\min(\alpha, F)$ has zeros of multiplicity one.
2. Any irreducible polynomial $f(x) \in F[x]$ is separable iff $f(x)$ has zeros of multiplicity one.

Proof of (1): Note that $[F(\alpha) : F] = \deg \min(\alpha, F)$, and $\{F(\alpha) : F\}$ is the number of distinct zeros of $\min(\alpha, F)$.

Since all zeros have multiplicity 1, we have $[F(\alpha) : F] = \{F(\alpha) : F\}$.

■

Proof of (2): If $f(x) \in F[x]$ is irreducible and $\alpha \in \overline{F}$ a root, then $\min(\alpha, F) \mid f(\alpha)$.

But then $f(x) = \ell \min(\alpha, F)$ for some constant $\ell \in F$, since $\min(\alpha, F)$ was monic and only had zeros of multiplicity one.

■

Theorem: If $K \geq E \geq F$ and $[K : F] < \infty$, then K is separable over F iff K is separable over E and E is separable over F.

Proof:

$$\begin{aligned} [K : F] &= [K : E][E : F] \\ &= \{K : E\}\{E : F\} \\ &= \{K : F\}. \end{aligned}$$

Corollary: Let $E \geq F$ be a finite extension. Then

$$E \text{ is separable over } F \iff \text{Every } \alpha \in E \text{ is separable over } F.$$

Proof:

$\implies$: Suppose $E \geq F$ is separable.

Then $E \geq F(\alpha) \geq F$ implies that $F(\alpha)$ is separable over F and thus α is separable.

$\impliedby$: Suppose every $\alpha \in E$ is separable over F.

Since $E = F(\alpha_1, \cdots, \alpha_n)$, build a tower of extensions over F. For the first step, consider $F(\alpha_1, \alpha_2) \to F(\alpha_1) \to F$.

We know $F(\alpha_1)$ is separable over F. To see that $F(\alpha_1, \alpha_2)$ is separable over $F(\alpha_1)$, consider α_2.

α_2 is separable over $F \iff \min(\alpha_2, F)$ has roots of multiplicity one.

Then $\min(\alpha_2, F(\alpha_1)) \mid \min(\alpha_2, F)$, so $\min(\alpha_2, F(\alpha))$ has roots of multiplicity one.

Thus $F(\alpha_1, \alpha_2)$ is separable over $F(\alpha_1)$.

■

14.1 Perfect Fields

Lemma: $f(x) \in F[x]$ has a multiple root $\iff$ $f(x), f'(x)$ have a nontrivial (multiple) common factor.

Proof:

$\implies$: Let $K \geq F$ be an extension field of F.

Suppose $f(x), g(x)$ have a common factor in $K[x]$; then f, g also have a common factor in $F[x]$.

If f, g do not have a common factor in $F[x]$, then $\gcd(f, g) = 1$ in $F[x]$, and we can find $p(x), q(x) \in F[x]$ such that $f(x)p(x) + g(x)q(x) = 1$.

But this equation holds in $K[x]$ as well, so $\gcd(f, g) = 1$ in $K[x]$.

We can therefore assume that the roots of f lie in F. Let $\alpha \in F$ be a root of f. Then

$$
\begin{aligned}
f(x) &= (x-\alpha)^m g(x) \\
f'(x) &= m(x-\alpha)^{m-1} g(x) + (x-\alpha)^m g'(x).
\end{aligned}
$$

If α is a multiple root, $m > 2$, and thus $(x - \alpha) \mid f'$.

$\impliedby$: Suppose f does not have a multiple root.

We can assume all of the roots are in F, so we can split f into linear factors.

So

$$
\begin{aligned}
f(x) &= \prod_{i=1}^{n} (x - \alpha_i) \\
f'(x) &= \sum_{i=1}^{n} \prod_{j \neq i} (x - \alpha_j).
\end{aligned}
$$

But then $f'(\alpha_k) = \prod j \neq k(x - \alpha_j) \neq 0$. Thus f, f' can not have a common root.

$\blacksquare$

Moral: we can thus test separability by taking derivatives.

Definition: A field F is *perfect* if every finite extension of F is separable.

Theorem: Every field of characteristic zero is perfect.

Proof: Let F be a field with $\text{char}(F) = 0$, and let $E \geq F$ be a finite extension.

Let $\alpha \in E$, we want to show that α is separable. Consider $f = \min(\alpha, F)$. We know that f is irreducible over F, and so its only factors are $1, f$. If f has a multiple root, then f, f' have a common factor in $F[x]$. By irreducibility, $f \mid f'$, but $\deg f' < \deg f$, which implies that $f'(x) = 0$. But this forces $f(x) = c$ for some constant $c \in F$, which means f has no roots – a contradiction.

So α separable for all $\alpha \in E$, so E is separable over F, and F is thus perfect.

■

Theorem: Every finite field is perfect.

Proof: Let F be a finite field with $\mathrm{char} F = p > 0$ and let $E \geq F$ be finite. Then $E = F(\alpha)$ for some $\alpha \in E$, since E is a simple extension (look at E^*?) So E is separable over F iff $\min(\alpha, F)$ has distinct roots.

So $E^\times = E \setminus \{0\}$, and so $|E| = p^n \implies |E| = p^{n-1}$. Thus all elements of E satisfy

$$f(x) := x^{p^n} - x \in \mathbb{Z}_p[x].$$

So $\min(\alpha, F) \mathrel{\Big|} f(x)$. One way to see this is that *every* element of E satisfies f, since there are exactly p^n distinct roots.

Another way is to note that

$$f'(x) = p^n x^{p^n - 1} - 1 = -1 \neq 0.$$

Since $f(x)$ has no multiple roots, $\min(\alpha, F)$ can not have multiple roots either.

■

Note that $[E : F] < \infty \implies F(\alpha_1, \cdots, \alpha_n)$ for some $\alpha_i \in E$ that are algebraic over F.

14.2 Primitive Elements

Theorem (Primitive Element): Let $E \geq F$ be a finite extension and separable.

Then there exists an $\alpha \in E$ such that $E = F(\alpha)$.

Proof: See textbook.

Corollary: Every finite extension of a field of characteristic zero is simple.

15 Tuesday October 8th

15.1 Splitting Fields

For $\overline{F} \geq E \geq F$, we can use the lifting theorem to get a $\tau : E \to E'$. What conditions guarantee that $E = E'$?

If $E = F(\alpha)$, then $E' = F(\beta)$ for some β a conjugate of α. Thus we need E to contain conjugates of all of its elements.

Definition: Let $\left\{ f_i(x) \in F[x] \mathrel{\Big|} i \in I \right\}$ be any collection of polynomials. We way that E is a **splitting field** $\iff$ E is the smallest subfield of $\overline{F}$ containing all roots of the f_i.

Examples:

- $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field for $\left\{ x^{-}2, x^2 - 5 \right\}$.

- $\mathbb{C}$ is a splitting field for $\left\{x^2+1\right\}$.
- $\mathbb{Q}(\sqrt[3]{2})$ is *not* a splitting field for any collection of polynomials.

Theorem: Let $F \leq E \leq \overline{F}$. Then E is a splitting field over F for some set of polynomials $\iff$ every isomorphism of E fixing F is in fact an automorphism.

Proof:

$\implies$: Let E be a splitting field of $\left\{f_i(x) \;\middle|\; f_i(x) \in F[x], i \in I\right\}$.

Then $E = \left\langle \alpha_j \;\middle|\; j \in J\right\rangle$ where α_j are the roots of all of the f_i.

Suppose $\sigma : E \to E'$ is an isomorphism fixing F. Then consider $\sigma(\alpha_j)$ for some $j \in J$. We have

$$\min(\alpha, F) = p(x) = a_0 + a_1 x + \cdots a_{n-1}x^{n-1} + a_n x^n,$$

and so

$$p(x) = 0,\ 0 \in F \implies 0 = \sigma(p(\alpha_j)) = \sum_i a_i \sigma(\alpha_j)^i.$$

Thus $\sigma(\alpha_j)$ is a conjugate, and thus a root of some $f_i(x)$.

$\impliedby$: Suppose any isomorphism of E leaving F fixed is an automorphism.

Let $g(x)$ be an irreducible polynomial and $\alpha \in E$ a root.

$$
\begin{tikzcd}
\overline{F} & & \overline{F} \\
E \arrow[rr, dash, "\sim"] \arrow[d, dash] & & E' = E \arrow[u, dash] \arrow[d, dash] \\
F(\alpha) \arrow[rr, dash] \arrow[d, dash] & & F(\beta) \arrow[d, dash] \\
F \arrow[rr, dash] & & F
\end{tikzcd}
$$

Using the lifting theorem, where $F(\alpha \leq E$, we get a map $\tau : E \to E'$ lifting the identity and the conjugation homomorphism. But this says that E' must contain every conjugate of α.

Therefore we can take the collection

$$S = \left\{ g_i(x) \in F[x] \;\middle|\; g_i \text{ irreducible and has a root in } E \right\}.$$

This defines a splitting field for $\{g_j\}$, and we're done.

$\blacksquare$

Examples:

1. $x^2 + 1 \in \mathbb{R}[x]$ splits in $\mathbb{C}$, i.e. $x^2 + 1 = (x+i)(x-i)$.
2. $x^2 - 2 \in \mathbb{Q}[x]$ splits in $\mathbb{Q}(\sqrt{2})$.

Corollary: Let E be a splitting field over F. Then every **irreducible** polynomial in $F[x]$ with a root $\alpha \in E$ splits in $E[x]$.

Corollary: The index $\{E : F\}$ (the number of distinct lifts of the identity). If E is a splitting field and $\tau : E \to E'$ lifts the identity on F, then $E = E'$. Thus $\{E : F\}$ is the number of automorphisms, i.e. $|\mathrm{Gal}(E/F)|$.

Question: When is it the case that

$$[E : F] = \{E : F\} = |\mathrm{Gal}(E/F)|?$$

- The first equality occurs when E is separable.
- The second equality occurs when E is a splitting field.

Characteristic zero implies separability

Definition: If E satisfies both of these conditions, it is said to be a **Galois extension**.

Some cases where this holds:

- $E \geq F$ a finite algebraic extension with E characteristic zero.
- E a finite field, since it is a splitting field for $x^{p^n} - x$.

Example 1: $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ is

1. A degree 4 extension,
2. The number of automorphisms was 4, and
3. The Galois group was $\mathbb{Z}_2^2$, of size 4.

Example 2: E the splitting field of $x^3 - 3$ over $\mathbb{Q}$.

This polynomial has roots $\sqrt[3]{3},\ \zeta_3 \sqrt[3]{3},\ \zeta_3^2 \sqrt[3]{3}$ where $\zeta_3^3 = 1$.

Then $E = \mathbb{Q}(\sqrt[3]{3}, \zeta_3)$, where

$$\begin{aligned}
\min(\sqrt[3]{3}, \mathbb{Q}) &= x^3 - 3 \\
\min(\zeta_3, \mathbb{Q}) &= x^2 + x + 1,
\end{aligned}$$

so this is a degree 6 extension.

Since char $\mathbb{Q} = 0$, we have $[E : \mathbb{Q}] = \{E : \mathbb{Q}\}$ for free.

We know that any automorphism has to map

$$\begin{aligned}
\sqrt[3]{3} &\mapsto \sqrt[3]{3},\ \sqrt[3]{3}\zeta_3,\ \sqrt[3]{3}\zeta_3^2 \\
\zeta_3 &\mapsto \zeta_3,\ \zeta_3^2.
\end{aligned}$$

You can show this is nonabelian by composing a few of these, thus the Galois group is S^3.

Example 3 If $[E : F] = 2$, then E is automatically a splitting field.

Since it's a finite extension, it's algebraic, so let $\alpha \in E \setminus F$.

Then $\min(\alpha, F)$ has degree 2, and thus $E = F(\alpha)$ contains all of its roots, making E a splitting field.

15.2 The Galois Correspondence

There are three key players here:

$$[E : F], \quad \{E : F\}, \quad \mathrm{Gal}(E/F).$$

How are they related?

Definition: Let $E \geq F$ be a finite extension. E is **normal** (or Galois) over F iff E is a separable splitting field over F.

Examples:

1. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is normal over $\mathbb{Q}$.
2. $\mathbb{Q}(\sqrt[3]{3})$ is not normal (not a splitting field of any irreducible polynomial in $\mathbb{Q}[x]$).
3. $\mathbb{Q}(\sqrt[3]{3}, \zeta_3)$ is normal

Theorem: Let $F \leq E \leq K \leq \overline{F}$, where K is a finite normal extension of F. Then

1. K is a normal extension of E as well,
2. $\mathrm{Gal}(K/E) \leq \mathrm{Gal}(K/F)$.
3. For $\sigma, \tau \in \mathrm{Gal}(K/F)$,

$$\sigma \Big|_E = \tau \Big|_E \iff \sigma, \tau \text{ are in the same left coset of } \frac{\mathrm{Gal}(K/F)}{\mathrm{Gal}(K/E)}.$$

Proof of (1): Since K is separable over F, we have K separable over E.

Then K is a splitting field for polynomials in $F[x] \subseteq E[x]$. Thus K is normal over E.

$\blacksquare$

Proof of (2):

$$\begin{array}{ccc} K & \xrightarrow{\tau} & K \\ E & \xrightarrow{\mathrm{id}} & E \\ F & \xrightarrow{\mathrm{id}} & F \end{array}$$

So this follows by definition.

■

Proof of (3): Let $\sigma, \tau \in \mathrm{Gal}(K/F)$ be in the same left coset. Then

$$\tau^{-1}\sigma \in \mathrm{Gal}(K/E),$$

so let $\mu \coloneqq \tau^{-1}\sigma$.

Note that μ fixes E by definition.

So $\sigma = \tau\mu$, and thus

$$\sigma(e) = \tau(\mu(e)) = \tau(e) \text{ for all } e \in E.$$

$\blacksquare$

Note: We don't know if the intermediate field E is actually a *normal* extension of F.

Standard example: $K \geq E \geq F$ where

$$K = \mathbb{Q}(\sqrt[3]{3}, \zeta_3) \quad E = \mathbb{Q}(\sqrt[3]{3}) \quad F = \mathbb{Q}.$$

Then $K \trianglelefteq E$ and $K \trianglelefteq F$, since $\mathrm{Gal}(K/F) = S_3$ and $\mathrm{Gal}(K/E) = \mathbb{Z}_2$. But $E \ntrianglelefteq F$, since $\mathbb{Z}_2 \ntrianglelefteq S_3$.

16 Thursday October 10th

16.1 Computation of Automorphisms

Setup:

- $F \leq E \leq K \leq \overline{F}$
- $[K : F] < \infty$
- K is a normal extension of F

Facts:

- $\mathrm{Gal}(K/E) = \left\{ \sigma \in \mathrm{Gal}(K/F) \;\middle|\; \sigma(e) = e \ \forall e \in E \right\}$.
- $\sigma, \tau \in \mathrm{Gal}(K/F)$ and $\sigma|_E = \tau|_E \iff \sigma, \tau$ are in the same left coset of $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$.

Example: $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$.

Then $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2^2$, given by the following automorphisms:

$$\begin{aligned}
\mathrm{id} : \sqrt{2} \mapsto \sqrt{2}, &\qquad \sqrt{5} \mapsto \sqrt{5} \\
\rho_1 : \sqrt{2} \mapsto \sqrt{2}, &\qquad \sqrt{5} \mapsto -\sqrt{5} \\
\rho_2 : \sqrt{2} \mapsto -\sqrt{2}, &\qquad \sqrt{5} \mapsto \sqrt{5} \\
\rho_1 \circ \rho_2 : \sqrt{2} \mapsto -\sqrt{2}, &\qquad \sqrt{5} \mapsto -\sqrt{5}.
\end{aligned}$$

We then get the following subgroup/subfield correspondence:

$$
\begin{tikzcd}
 & \mathbb{Z}_2^2 & \\
\{\mathrm{id}, \rho_1\} \arrow[ur] & \{\mathrm{id}, \rho_2\} \arrow[u] & \{\mathrm{id}, \rho_1 \circ \rho_2\} \arrow[ul] \\
 & \{\mathrm{id}\} \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt{5}) \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr] & \mathbb{Q}(\sqrt{5}) \arrow[d] & {} \arrow[dl] \\
 & \mathbb{R} &
\end{tikzcd}
$$

16.2 Fundamental Theorem of Galois Theory

Recall that $:= \mathrm{Gal}(K/E)$.

Theorem (Fundamental Theorem of Galois Theory):

Let $\mathcal{D}$ be the collection of subgroups of $\mathrm{Gal}(K/F)$ and $\mathcal{C}$ be the collection of subfields E such that $F \leq E \leq K$.

Define a map

$$
\begin{aligned}
&\lambda : \mathcal{C} \to \mathcal{D} \\
&\lambda(E) := \left\{ \sigma \in \mathrm{Gal}(K/F) \;\middle|\; \sigma(e) = e \ \forall e \in E \right\}.
\end{aligned}
$$

Then λ is a bijective map, and

1. $\lambda(E) = \mathrm{Gal}(K/E)$
2. $E = K_{\lambda(E)}$
3. If $H \leq \mathrm{Gal}(K/F)$ then
$$\lambda(K_H) = H$$
4. $[K : E] = |\lambda(E)|$ and
$$[E : F] = [\mathrm{Gal}(K/F) : \lambda(E)]$$
5. E is normal over $F \iff \lambda(E) \trianglelefteq \mathrm{Gal}(K/F)$, and in this case
$$\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E).$$
6. λ is order-reversing, i.e.
$$E_1 \leq E_2 \implies \lambda(E_2) \leq \lambda(E_1).$$

Proof of 1: Proved earlier.

■

Proof of 2: We know that $E \leq L_{\mathrm{Gal}(K/E)}$. Let $\alpha \in K \setminus E$; we want to show that α is not fixed by all automorphisms in $\mathrm{Gal}(K/E)$.

We build the following tower:

$$
\begin{tikzcd}
K \arrow[r, dotted, "\tau'"] & K \\
E(\alpha) \arrow[u] \arrow[r, "\tau"] & E(\beta) \arrow[u] \\
E \arrow[u] \arrow[r, "\mathrm{id}"] & E \arrow[u] \\
F \arrow[u] \arrow[r, "\mathrm{id}"] & F \arrow[u]
\end{tikzcd}
$$

This uses the isomorphism extension theorem, and the fact that K is normal over F.

If $\beta \neq \alpha$, then β must be a conjugate of α, so $\tau'(\alpha) \neq \alpha$ while $\tau' \in \mathrm{Gal}(K/E)$.

■

Claim: λ is injective.
Proof: Suppose $\lambda(E_1) = \lambda(E_2)$. Then by (2), $E_1 = K_{\lambda(E_1)} = K_{\lambda(E_2)} = E_2$. ■

Proof of 3: We want to show that if $H \leq \mathrm{Gal}(K/F)$ then $\lambda(K_H) = H$.

We know $H \leq \lambda(K_H) = \mathrm{Gal}(K/K_H) \leq \mathrm{Gal}(K/F)$, so suppose $H \lneq \lambda(K_H)$.

Since K is a finite, separable extension, $K = K_H(\alpha)$ for some $\alpha \in K$.

Let

$$n = [K : K_H] = K : K_H = |\mathrm{Gal}(K/K_H)|.$$

Since $H \lneq \lambda(K_H)$, we have $|H| < n$. So denote $H = \{\sigma, \sigma_2, \cdots\}$ and let define

$$f(x) = \prod_i (x - \sigma_i(\alpha)).$$

We then have

- $\deg f = |H|$
- The coefficients of f are symmetric polynomials in the $\sigma_i(\alpha)$ and are fixed under any $\sigma \in H$
- $f(x) \in K_H(\alpha)[x]$
- $f(\alpha) = 0$ since $\sigma_i(\alpha) = \alpha$ for every i.

This is a contradiction, so we must have

$$[K_H : K] = n = \deg \min(\alpha, K_H) \leq \deg f = |H|.$$

■

Assuming (3), λ is surjective, so suppose $H < \mathrm{Gal}(K/F)$. Then $\lambda(K_H) = H \implies \lambda$ is surjective.

Proof of 4:

$$\begin{aligned}
|\lambda(E)| = |\mathrm{Gal}(K/E)| &\quad =_{\text{splitting field}} [K : E] \\
[E : F] =_{\text{separable}} \{E : F\} &\quad =_{\text{previous part}} [\mathrm{Gal}(K/F) : \lambda(E)].
\end{aligned}$$

Proof of 5:

We have $F \leq E \leq K$ and E is separable over F, so E is normal over $F \iff E$ is a splitting field over F.

That is, every extension E'/E maps K to itself, since K is normal.

$$\begin{tikzcd}
K & K \\
E \arrow[u] & E' \arrow[u] \\
F \arrow[u] \arrow[r, "id"] & F \arrow[u]
\end{tikzcd}$$

So E is normal over $F \iff$ for all $\sigma \in \mathrm{Gal}(K/F), \sigma(\alpha) \in E$ for all $\alpha \in E$.

By a previous property, $E = K_{\mathrm{Gal}(K/E)}$, and so

$$\begin{aligned}
\sigma(\alpha) \in E &\iff \tau(\sigma(\alpha)) = \sigma(\alpha) && \forall \tau \in \mathrm{Gal}(K/E) \\
&\iff (\sigma^{-1}\tau\sigma)(\alpha) = \alpha S && \forall \tau \in \mathrm{Gal}(K/E) \\
&\iff \sigma^{-1}\tau\sigma \in \mathrm{Gal}(K/E) \\
&\iff \mathrm{Gal}(K/E) \trianglelefteq \mathrm{Gal}(K/F).
\end{aligned}$$

Now assume E is a normal extension of F, and let

$$\begin{aligned}
\phi : \mathrm{Gal}(K/F) &\to \mathrm{Gal}(E/F) \\
\sigma &\mapsto \sigma|_E.
\end{aligned}$$

Then ϕ is well-defined precisely because E is normal over F, and we can apply the extension theorem:

$$\begin{tikzcd}
K & K \\
E \arrow[u] \arrow[r, "\tau"] & E \arrow[u] \\
F \arrow[u] \arrow[r, "\mathrm{id}"] & F \arrow[u]
\end{tikzcd}$$

ϕ is surjective by the extension theorem, and ϕ is a homomorphism, so consider $\ker \phi$.

Let $\phi(\sigma) = \sigma|_E = \mathrm{id}$. Then ϕ fixes elements of $E \iff \sigma \in \mathrm{Gal}(K/E)$, and thus $\ker \phi = \mathrm{Gal}(K/E)$.

■

Proof of 6:

$$\begin{array}{ccc} E_1 \leq E_2 \iff \mathrm{Gal}(K/E_2) \leq & & \mathrm{Gal}(K/E_1) \\ \shortparallel & & \shortparallel \\ \lambda(E_2) \leq & & \lambda(E_1). \end{array}$$

Example: $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Then $\min(\zeta, \mathbb{Q}) = x^2 + x + 1$ and $\mathrm{Gal}(K/\mathbb{Q}) = S_3$. There is a subgroup of order 2, $E = \mathrm{Gal}(K/\mathbb{Q}(\sqrt[3]{2})) \leq \mathrm{Gal}(K/\mathbb{Q})$, but E doesn't correspond to a normal extension of F, so this subgroup is not normal. On the other hand, $\mathrm{Gal}(\mathbb{Q}(\zeta_3), \mathbb{Q}) \trianglelefteq \mathrm{Gal}(K/\mathbb{Q})$.

17 Tuesday October 15th

17.1 Cyclotomic Extensions

Definition: Let K denote the splitting field of $x^n - 1$ over F. Then K is called the **nth cyclotomic extension of F**.

If we set $f(x) = x^n - 1$, then $f'(x) = nx^{n-1}$.

So if char F does not divide n, then the splitting field is separable. So this splitting field is in fact normal.

Suppose that char F doesn't divide n, then $f(x)$ has n zeros, and let ζ_1, ζ_2 be two zeros. Then $(\zeta_1\zeta_2)^n = \zeta_1^n\zeta_2^n = 1$, so the product is a zero as well, and the roots of f form a subgroup in $K^\times$.

So let's specialize to $F = \mathbb{Q}$.

The roots of f are the nth roots of unity, i.e. $\zeta_n = e^{2\pi i/n}$, and are given by $\left\{\zeta_n, \zeta_n^2, \zeta_n^3, \cdots, \zeta_n^{n-1}\right\}$.

The *primitive* roots of unity are given by $\left\{\zeta_n^m \;\middle|\; \gcd(m,n) = 1\right\}$.

Definition: Let

$$\Phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \alpha_i),$$

where this product runs over all of the primitive nth roots of unity.

Let G be $\mathrm{Gal}(K/\mathbb{Q})$. Then any $\sigma \in G$ will permute the primitive nth roots of unity. Moreover, it *only* permutes primitive roots, so every σ fixes $\Phi_n(x)$. But this means that the coefficients must lie in $\mathbb{Q}$.

Since ζ generates all of the roots of Φ_n, we in fact have $K = \mathbb{Q}(\zeta)$. But what is the group structure of G?

Since any automorphism is determined by where it sends a generator, we have automorphisms $\tau_m(\zeta) = \zeta^m$ for each m such that $\gcd(m,n) = 1$.

But then $\tau_{m_1} \circ \tau_{m_2} = \tau_{m_1+m_2}$, and so $G \cong G_m \leq \mathbb{Z}_n$ as a ring, where

$$G_m = \left\{[m] \;\middle|\; \gcd(m,n) = 1\right\}$$

and $|G| = \varphi(n)$.

Note that as a *set*, there are the units $\mathbb{Z}_n^\times$.

Theorem: The Galois group of the nth cyclotomic extension over $\mathbb{Q}$ has $\varphi(n)$ elements and is isomorphic to G_m.

Special case: $n = p$ where p is a prime.

Then $\phi(p) = p - 1$, and

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Note that $\mathbb{Z}_p^\times$ is in fact cyclic, although this may not always happen. In this case, we have $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_p^\times$.

17.2 Construction of n-gons

To construct the vertices of an n-gon, we will need to construct the angle $2\pi/n$, or equivalently, ζ_n. Note that if $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \neq 2^\ell$ for some $\ell \in \mathbb{N}$, then the n-gon is *not* constructible.

Example: An 11-gon. Noting that $[\mathbb{Q}(\zeta_{11}) : \mathbb{Q}] = 10 \neq 2^\ell$, the 11-gon is not constructible.

Since this is only a sufficient condition, we'll refine this.

Definition: A prime of the form $p = 2^{2^k} + 1$ are called **Fermat primes**.

Theorem: The regular n-gon is constructible $\iff$ all odd primes dividing n are *Fermat primes* p where p^2 does not divide n.

Example: Consider

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1.$$

Then take $\zeta = \zeta_5$; we then obtain the roots as $\left\{1, \zeta, \zeta^2, \zeta^3, \zeta^4\right\}$ and $\mathbb{Q}(\zeta)$ is the splitting field.

Any automorphism is of the form $\sigma_r : \zeta \mapsto \zeta^r$ for $r = 1, 2, 3, 4$. So $|\mathrm{Gal}(K/\mathbb{Q})| = 4$, and is cyclic and thus isomorphic to $\mathbb{Z}_4$. Corresponding to $0 \to \mathbb{Z}_2 \to \mathbb{Z}_4$, we have the extensions

$$\mathbb{Q} \to \mathbb{Q}(\zeta^2) \to \mathbb{Q}(\zeta).$$

How can we get a basis for the degree 2 extension $\mathbb{Q}(\zeta^2)/\mathbb{Q}$? Let

$$\lambda(E) = \left\{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \;\middle|\; \sigma(e) = e \;\forall e \in E\right\},$$

$\lambda(K_H) = H$ where H is a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, and

$$K_H = \left\{x \in K \;\middle|\; \sigma(x) = x \;\forall \sigma \in H\right\}.$$

Note that if $\mathbb{Z}_4 = \langle \psi \rangle$, then $\mathbb{Z}_2 \leq \mathbb{Z}_4$ is given by $\mathbb{Z}_2 = \left\langle \psi^2 \right\rangle$.

We can compute that if $\psi(\zeta) = \zeta^2$, then

$$\begin{aligned}\psi^2(\zeta) &= \zeta^{-1}\\ \psi^2(\zeta^2) &= \zeta^{-2}\\ \psi^2(\zeta^3) &= \zeta^{-3}.\end{aligned}$$

Noting that ζ_4 is a linear combination of the other ζs, we have a basis $\left\{1, \zeta, \zeta^2, \zeta^3\right\}$.

Then you can explicitly compute the fixed field by writing out

$$\sigma(a + b\zeta + c\zeta^2 + d\zeta^3) = a + b\sigma(\zeta) + c\sigma(\zeta^2) + \cdots,$$

gathering terms, and seeing how this restricts the coefficients.

In this case, it yields $\mathbb{Q}(\zeta^2 + \zeta^3)$.

17.3 The Frobenius Automorphism

Definition: Let p be a prime and F be a field of characteristic $p > 0$. Then

$$\begin{aligned}\sigma_p &: F \to F\\ \sigma_p(x) &= x^p\end{aligned}$$

is denoted the *Frobenius map.*

Theorem: Let F be a finite field of characteristic $p > 0$. Then

1. ϕ_p is an automorphism, and
2. ϕ_p fixes $F_{\sigma_p} = \mathbb{Z}_p$.

Proof of part 1: Since σ_p is a field homomorphism, we have

$$\sigma_p(x + y) = (x + y)^p = x^p + y^p \text{ and } \sigma(xy) = (xy)^p = x^p y^p$$

Note that σ_p is injective, since $\sigma_p(x) = 0 \implies x^p = 0 \implies x = 0$ since we are in a field. Since F is finite, σ_p is also surjective, and is thus an automorphism.

Proof of part 2: If $\sigma(x) = x$, then

$$x^p = x \implies x^p - x = 0,$$

which implies that x is a root of $f(x) = x^p - x$. But these are exactly the elements in the prime ring $\mathbb{Z}_p$.

■

18 Thursday October 17th

18.1 Example Galois Group Computation

Example: What is the Galois group of $x^4 - 2$ over $\mathbb{Q}$?

First step: find the roots. We can find directly that there are 4 roots given by

$$\left\{ \pm \sqrt[4]{2}, \pm i \sqrt[4]{2} \right\} \coloneqq \{r_i\}.$$

The splitting field will then be $\mathbb{Q}(\sqrt[4]{2}, i)$, which is separable because we are in characteristic zero. So this is a normal extension.

We can find some automorphisms:

$$\sqrt[4]{2} \mapsto r_i, \quad i \mapsto \pm i.$$

So $|G| = 8$, and we can see that G can't be abelian because this would require every subgroup to be abelian and thus normal, which would force every intermediate extension to be normal.

But the intermediate extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not a normal extension since it's not a splitting field.

So the group must be D_4.

$\blacksquare$

18.2 Insolubility of the Quintic

18.2.1 Symmetric Functions

Let F be a field, and let

$$F(y_1, \cdots, y_n) = \left\{ \frac{f(y_1, \cdots, y_n)}{g(y_1, \cdots, y_n)} \mathrel{\Big|} f, g \in F[y_1, \cdots, y_n] \right\}$$

be the set of *rational* functions over F.

Then $S_n \curvearrowright F(y_1, \cdots, y_n)$ by permuting the y_i, i.e.

$$\sigma \left(\frac{f(y_1, \cdots, y_n)}{g(y_1, \cdots, y_n)} \right) = \frac{f(\sigma(y_1), \cdots, \sigma(y_n))}{g(\sigma(y_1), \cdots, \sigma(y_n))}.$$

Definition: A function $f \in F(\alpha_1, \cdots, \alpha_n)$ is **symmetric** $\iff$ under this action, $\sigma \curvearrowright f = f$ for all $\sigma \in S_n$.

Examples:

1. $f(y_1, \cdots, y_n) = \prod y_i$
2. $f(y_1, \cdots, y_n) = \sum y_i$.

18.2.2 Elementary Symmetric Functions

Consider $f(x) \in F(y_1, \cdots, y_n)[x]$ given by $\prod(x - y_i)$. Then $\sigma f = f$, so f is a symmetric function. Moreover, all coefficients are fixed by S_n. So the coefficients themselves are symmetric functions.

Concretely, we have

Coefficient	Term
1	$(-1)^n$
x^{n-1}	$-y_1 - y_2 - \cdots - y_n$
x^{n-2}	$y_1y_2 + y_1y_3 + \cdots + y_2y_3 + \cdots$

The coefficient of x^{n-i} is referred to as the *ith elementary symmetric function.*

Consider an intermediate extension E given by joining all of the elementary symmetric functions:

$$
\begin{tikzcd}
F(y_1, \cdots, y_n) \arrow[d, dash] \\
K \arrow[d, dash] \\
E = F(s_1, \cdots, s_n) \arrow[d, dash] \\
F
\end{tikzcd}
$$

Let K denote the base field with *all* symmetric functions adjoined; then K is an intermediate extension, and we have the following results:

Theorem:

1. $E \leq K$ is a field extension.

2. $E \leq F(y_1, \cdots, y_n)$ is a finite, normal extension since it is the splitting field of $f(x) = \prod(x - y_i)$, which is separable.

We thus have

$$[F(y_1, \cdots, y_n) : E] \leq n! < \infty.$$

Proof:

We'll show that in fact $E = K$, so all symmetric functions are generated by the elementary symmetric functions.

By definition of symmetric functions, K is exactly the fixed field $F(y_1, \cdots, y_n)_{S_n}$, and $|S|_n = n!$.

So we have

$$\begin{aligned} n! &= |\mathrm{Gal}(F(y_1, \cdots, y_n/K))| \\ &\leq \{F(y_1, \cdots, y_n) : K\} \\ &\leq [F(y_1, \cdots, y_n) : K]. \end{aligned}$$

But now we have

$$n! \leq [F(y_1, \cdots, y_n) : K] \leq [F(y_1, \cdots, y_n) : E] \leq n!$$

which forces $K = E$.

■

Theorem:

1. Every symmetric function can be written as a combination of sums, products, and possibly quotients of elementary symmetric functions.
2. $F(y_1, \cdots, y_n)$ is a finite normal extension of $F(s_1, \cdots, s_n)$ of degree $n!$.
3. $\mathrm{Gal}(F(y_1, \cdots, y_n)/F(s_1, \cdots, s_n)) \cong S_n$.

We know that every group $G \hookrightarrow S_n$ by Cayley's theorem. So there exists an intermediate extension

$$F(s_1, \cdots, s_n) \leq L \leq F(y_1, \cdots, y_n)$$

such that $G = \mathrm{Gal}(F(y_1, \cdots, y_n)/L)$.

> Open question: which groups can be realized as Galois groups over $\mathbb{Q}$? Old/classic question, possibly some results in the other direction (i.e. characterizations of which groups *can't* be realized as such Galois groups).

18.2.3 Extensions by Radicals

Let $p(x) = \sum a_i x^i \in \mathbb{Q}[x]$ be a polynomial of degree n. Can we find a formula for the roots as a function of the coefficients, possibly involving radicals?

- For $n = 1$ this is clear

- For $n = 2$ we have the quadratic formula.
- For $n = 3$, there is a formula by work of Cardano.
- For $n = 4$, this is true by work of Ferrari.
- For $n \geq 5$, there can **not** be a general equation.

Definition: Let $K \geq F$ be a field extension. Then K is an **extension of F by radicals** (or a **radical extension**) $\iff$ $K = \alpha_1, \cdots, \alpha_n$ for some α_i such that

1. Each $\alpha_i^{m_i} \in F$ for some $m_i > 0$.
2. For each i, $\alpha_i^{\ell_i} \in F(\alpha_1, \cdots, \alpha_{i-1})$ for some $\ell_i < m_i$ (?).

Definition: A polynomial $f(x) \in F[x]$ is **solvable by radicals** over $F \iff$ the splitting field of f is contained in some radical extension.

Example: Over $\mathbb{Q}$, the polynomials $x^5 - 1$ and $x^3 - 2$ are solvable by radicals.

Recall that G is *solvable* if there exists a normal series

$$1 \trianglelefteq H_1 \trianglelefteq H_2 \cdots \trianglelefteq H_n \trianglelefteq G \text{ such that } H_n/H_{n-1} \text{ is abelian } \forall n.$$

18.2.4 The Splitting Field of $x^n - a$ is Solvable

Lemma: Let char $F = 0$ and $a \in F$. If K is the splitting field of $p(x) = x^n - a$, then $\mathrm{Gal}(K/F)$ is a solvable group.

Example: Let $p(x) = x^4 - 2/\mathbb{Q}$, which had Galois group D_4.

Proof: Suppose that F contains all nth roots of unity, $\left\{1, \zeta, \zeta^2, \cdots, \zeta^[n-1]\right\}$ where ζ is a primitive nth root of unity. If β is any root of $p(x)$, then $\zeta^i\beta$ is also a root for any $1 \leq i \leq n-1$. This in fact yields n distinct roots, and is thus all of the them. Since the splitting field K is of the form $F(\beta)$, then if $\sigma \in \mathrm{Gal}(K/F)$, then $\sigma(\beta) = \zeta^i\beta$ for some i. Then if $\tau \in \mathrm{Gal}(K/F)$ is any other automorphism, then $\tau(\beta) = \zeta^k\beta$ and thus (exercise) the Galois group is abelian and thus solvable.

Suppose instead that F does not contain all nth roots of unity. So let $F' = F(\zeta)$, so $F \leq F(\zeta) = F' \leq K$. Then $F \leq F(\zeta)$ is a splitting field (of $x^n - 1$) and separable since we are in characteristic zero and this is a finite extension. Thus this is a normal extension.

We thus have $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/F(\zeta)) \cong \mathrm{Gal}(F(\zeta)/F)$. We know that $\mathrm{Gal}(F(\zeta)/F)$ is abelian since this is a cyclotomic extension, and so is $\mathrm{Gal}(K/F(\zeta))$. We thus obtain a normal series

$$1 \trianglelefteq \mathrm{Gal}(K/F(\zeta)) \trianglelefteq \mathrm{Gal}(K/F)$$

Thus we have a solvable group.

■

19 Tuesday October 22nd

19.1 Certain Radical Extensions are Solvable

Recall the definition of an extension being *radical* (see above).

We say that a polynomial $f(x) \in K[x]$ is *solvable by radicals* iff its splitting field L is a radical extension of K.

Lemma: Let F be a field of characteristic zero.

If K is a splitting field of $f(x) = x^n - a \in F[x]$, then $\mathrm{Gal}(K/F)$ is a solvable group.

Theorem: Let F be characteristic zero, and suppose $F \leq E \leq K \leq \overline{F}$ be algebraic extension where E/F is normal and K a radical extension of F. Moreover, suppose $[K : F] < \infty$.

Then $\mathrm{Gal}(E/F)$ is solvable.

Proof: The claim is that K is contained in some L where $F \subset L$, L is a finite normal radical extension, and $\mathrm{Gal}L/F$ is solvable.

Since K is a radical extension of F, we have $F = K(\alpha_1, \cdots, \alpha_n)$ and $\alpha_i^{n_i} \in K(\alpha_1, \cdots, \alpha_{i-1})$ for each i and some $n_i \in \mathbb{N}$.

Let L_1 be the splitting field of $f_1(x) = x^{n_1} - \alpha_1^{n_1}$, then by the previous lemma, L_1 is a normal extension and $\mathrm{Gal}(L_1/F)$ is a solvable group.

Inductively continue this process, and letting

$$f_2(x) = \prod_{\sigma \in \mathrm{Gal}(L_1/F)} x^{n_2} - \sigma(\alpha_2)^{n_2} \in F[x].$$

Note that the action of the Galois group on this polynomial is stable. Let L_2 be the splitting field of f_2, then L_2 is a finite normal radical extension.

Then

$$\frac{\mathrm{Gal}(L_2/F)}{\mathrm{Gal}(L_2/L_1)} \cong \mathrm{Gal}(L_1/F),$$

which is solvable, and the denominator in this quotient is solvable, so the total group must be solvable as well. ■

19.2 Proof: Insolubility of the Quintic

Theorem (Insolubility of the quintic): Let $y_1, \cdots, y_n$ be independent transcendental elements in $\mathbb{R}$, then the polynomial $f(x) = \prod(x - y_i)$ is not solvable by radicals over $\mathbb{Q}(s_1, \cdots, s_n)$ where the s_i are the elementary symmetric polynomials in y_i.

So there are no polynomial relations between the transcendental elements.

Proof:

Let $n \geq 5$ and suppose y_i are transcendental over $\mathbb{R}$ and linearly independent over $\mathbb{Q}$. Then consider

$$\begin{aligned} s_1 &= \sum y_i \\ s_2 &= \sum_{i \leq j} y_i y_j \\ \cdots & \\ s_n &= \prod_i y_i. \end{aligned}$$

Then $\mathbb{Q}(y_1, \cdots, y_n)/\mathbb{Q}(s_1, \cdots, s_n)$ would be a normal extension precisely if $A_n \trianglelefteq S_n$ (by previous theorem). For $n \geq 5$, A_n is simple, and thus S_n is not solvable in this range.

Thus the polynomial is not solvable by radicals, since the splitting field of $f(x)$ is $\mathbb{Q}(y_1, \cdots, y_n)$. ■

19.3 Rings and Modules

Recall that a ring is given by $(R, +, \cdot)$, where

1. $(R, +)$ is an abelian group,
2. $(R, \cdot)$ is a monoid,
3. The distributive laws hold.

An *ideal* is certain type of subring that allows taking quotients, and is defined by $I \trianglelefteq R \iff I \leq R$ and $RI, IR \subseteq I$. The quotient is given by $R/I = \left\{ r + I \;\middle|\; r \in R \right\}$, and the ideal property is what makes this well-defined.

Much like groups, we have some notion of homomorphism $\phi : R \to R'$, where $\phi(ax + y) = \phi(a)\phi(x) + \phi(y)$.

19.3.1 Modules

We want to combine the following two notions:

- Groups acting on sets, and
- Vector spaces

Definition: Let R be a ring and M an abelian group. Then if there is a map

$$\begin{aligned} R \times M &\to M \\ (r, m) &\mapsto rm. \end{aligned}$$

such that $\forall s, r_1, r_2 \in R$ and $m_1, m_2 \in M$ we have

- $(sr_1 + r_2)(m_1 + m_2) = sr_1 m_1 + sr_1 m_2 + r_2 m_1 + r_2 m_2$
- $1 \in R \implies 1m = m.$

then M is said to be an R**-module.**

> Think of R like the group acting by scalar multiplication, and M the set of vectors with vector addition.

Examples:

1. $R = k$ a field, then a k-module is a vector space.
2. $R = G$ an abelian group, then R is a $\mathbb{Z}$-module where

$$n \curvearrowright a := \sum_{i=1}^{n} a.$$

> (In fact, these two notions are equivalent.)

3. $I \trianglelefteq R$, then $M \coloneqq R/I$ is an ring, which has an underlying abelian group, so M is an R-module where

$$M \curvearrowleft R = r \curvearrowright (s+I) \coloneqq (rs) + I.$$

4. For M an abelian group, $R \coloneqq \mathrm{End}(M) = \hom_{\mathbf{AbGrp}}(M, M)$ is a ring, and M is a left R-module given by

$$f \curvearrowright m \coloneqq f(m).$$

Definition: Let M, N be left R-modules. Then $f : M \to N$ is an R-module homomorphism $\iff$

$$f(rm_1 + m_2) = rf(m_1) + f(m_2).$$

Definition: *Monomorphisms* are injective maps, *epimorphisms* are surjections, and *isomorphisms* are both.

Definition: A *submodule* $N \leq M$ is a subset that is closed under all module operations.

We can consider images, kernels, and inverse images, so we can formulate homomorphism theorems analogous to what we saw with groups/rings:

Theorem:

1. If $M \xrightarrow{f} N$ in R-mod, then

$$M/\ker(f) \cong \mathrm{im}\,(f).$$

2. Let $M, N \leq L$, then $M + N \leq L$ as well, and

$$\frac{M}{M \bigcap N} \cong \frac{M+N}{N}.$$

3. If $M \leq M \leq L$, then

$$\frac{M}{N} \cong \frac{L/M}{L/N}$$

> Note that we can always quotient, since there's an underlying abelian group, and thus the "normality"/ideal condition is always satisfied for submodules. Just consider
>
> $$M/N \coloneqq \left\{ m + N \,\middle|\, m \in M \right\},$$
>
> then $R \curvearrowright (M/N)$ in a well-defined way that gives M/N the structure of an R-module as well.

20 Thursday October 24

20.1 Conjugates

Let $E \geq F$. Then $\alpha, \beta \in E$ are **conjugate** iff $\min(\alpha, F) = \min(\beta, F)$.

Example: $\alpha \pm bi \in \mathbb{C}$.

Theorem: Let F be a field and $\alpha, \beta \in F$ with $\deg \min(\alpha, F) = \deg \min(\beta, F)$, so

$$[F(\alpha) : F] = [F(\beta) : F].$$

Then α, β are conjugates $\iff$ $F(\alpha) \cong F(\beta)$ under the *conjugation map*,

$$\begin{aligned}\psi : F(\alpha) &\to F(\beta) \\ \sum_{i=1}^{n-1} a_i \alpha^i &\mapsto \sum_{i=1}^{n-1} a_i \beta^i.\end{aligned}$$

Proof:

$\Longleftarrow$:

Suppose that ψ is an isomorphism. Let $\min(\alpha, F) = p(x) = \sum c_i x^i$ where each $c_i \in F$. Then

$$0 = \psi(0) = \psi(p(\alpha)) = p(\beta) \implies \min(\beta, F) \;\Big|\; \min(\alpha, F).$$

Applying the same argument to $q(x) = \min(\beta, F)$ yields $\min(\beta, F) = \min(\alpha, F)$.

$\Longrightarrow$:

Suppose α, β are conjugates.

Exercise: Check that ψ is surjective and

$$\begin{aligned}\psi(x + y) &= \psi(x) + \psi(y) \\ \psi(xy) &= \psi(x)\psi(y).\end{aligned}$$

Let $z = \sum a_i \alpha^i$. Supposing that $\psi(z) = 0$, we have $\sum a_i \beta^i = 0$. By linear independence, this forces $a_i = 0$ for all i, and thus $z = 0$. So ψ is injective.

■

Corollary: Let $\alpha \in \overline{F}$ be algebraic. Then

1. Any $\phi : F(\alpha) \hookrightarrow \overline{F}$ such that $\phi(f) = f$ for all $f \in F$ must map α to a conjugate.
2. If $\beta \in \overline{F}$ is a conjugate of α, then there exists an isomorphism $\phi : F(\alpha) \to F(\beta) \subseteq \overline{F}$ such that $\phi(f) = f$ for all $f \in F$.

Proof of 1:

Let $\min(\alpha, F) = p(x) = \sum a_i x^i$. Note that $0 = \psi(p(\alpha)) = p(\psi(\alpha))$, and since p was irreducible, p must also be the minimal polynomial of $\psi(\alpha)$. Thus $\psi(\alpha)$ is a conjugate of α.

■

Proof of 2:

$F(\alpha)$ is generated by F and α, and ψ is completely determined by where it sends F and α. This shows uniquness.

$\blacksquare$

Corollary: Let $f(x) \in \mathbb{R}[x]$ and suppose $f(a+bi) = 0$. Then $f(a-bi) = 0$.

Proof: Both $i, -i$ are conjugates and $\min(i, \mathbb{R}) = \min(-i, \mathbb{R}) = x^2 + 1 \in \mathbb{R}[x]$. We then have a map

$$\psi : \mathbb{R}[i] \to \mathbb{R}[-i]$$
$$\psi(a+bi) = a + b(-i).$$

So if $f(a+bi) = 0$, then $0 = \psi(f(a+bi)) = f(\psi(a+bi)) = f(a-bi)$.

$\blacksquare$

21 Tuesday October 29th

21.1 Exact Sequences

Lemma (Short Five):

Consider a diagram of the following form:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "\alpha"] & N \arrow[r, "g"] \arrow[d, "\beta"] & Q \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & M' \arrow[r, "f'"] & N' \arrow[r, "g'"] & Q' \arrow[r] & 0
\end{tikzcd}$$

1. α, γ monomorphisms implies β is a monomorphism.
2. α, γ epimorphisms implies β is an epimorphism.
3. α, γ isomorphisms implies β is an isomorphism.

Moreover, (1) and (2) together imply (3).

Proof: Exercise.

Example proof of (2): Suppose α, γ are monomorphisms.

- Let $n \in N$ with $\beta(n) = 0$, then $g' \circ \beta(n) = 0$.
- $\implies \gamma \circ g(n) = 0$.
- $\implies g(n) = 0$
- $\implies \exists m \in M$ such that $f(m) = n$
- $\implies \beta \circ f(m) = \beta(n)$
- $\implies f'\alpha(m) = \beta(n) = 0$
- $\implies \alpha(m) = 0$
- $\implies f'$ is injective, so $m = 0$ and $n = f(m) = 0$.

$\blacksquare$

Definition: Two exact sequences are *isomorphic* iff in the following diagram, f, g, h are all isomorphisms:

$$
\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, "f"] & N \arrow[r] \arrow[d, "g"] & Q \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & M \arrow[r] & N \arrow[r] & Q \arrow[r] & 0
\end{tikzcd}
$$

Theorem: Let $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ be a SES. Then TFAE:

- There exists an R-module homomorphisms $h : M_3 \to M_2$ such that $g \circ h = \mathrm{id}_{M_3}$.
- There exists an R-module homomorphisms $k : M_2 \to M_1$ such that $k \circ f = \mathrm{id}_{M_1}$.
- The sequence is isomorphic to $0 \to M_1 \to M_1 \oplus M_3 \to M_3 \to 0$.

Proof: Define $\phi : M_1 \oplus M_3 \to M_2$ by $\phi(m_1 + m_2) = f(m_1) + h(m_2)$. We need to show that the following diagram commutes:

$$
\begin{tikzcd}
0 \arrow[r] & M_1 \arrow[r] \arrow[d, leftrightarrow, "\mathrm{id}"] & M_1 \oplus M_3 \arrow[r] & M_3 \arrow[r] \arrow[d, leftrightarrow, "\mathrm{id}"] & 0 \\
0 \arrow[r] & M_1 \arrow[r] & M_2 \arrow[r] \arrow[u, "\phi"] & M_3 \arrow[r] & 0
\end{tikzcd}
$$

We can check that

$$(g \circ \phi)(m_1 + m_2) = g(f(m_1)) + g(h(m_2)) = m_2 = \pi(m_1 + m_2).$$

This yields $1 \implies 3$, and $2 \implies 3$ is similar.

To see that $3 \implies 1, 2$, we attempt to define k, h in the following diagram:

$$
\begin{tikzcd}
0 \arrow[r] & M_1 \arrow[r] \arrow[d, leftrightarrow, "\mathrm{id}"] & M_1 \oplus M_3 \arrow[r] \arrow[l, bend right, "\pi_1"'] & M_3 \arrow[r] \arrow[d, leftrightarrow, "\mathrm{id}"] \arrow[l, bend right, "\iota_2"'] & 0 \\
0 \arrow[r] & M_1 \arrow[r] & M_2 \arrow[r] \arrow[u, "\phi"] \arrow[l, bend left, "k"] & M_3 \arrow[r] \arrow[l, bend left, "h"] & 0
\end{tikzcd}
$$

So define $k = \pi_1 \circ \phi^{-1}$ and $h = \phi \circ \iota_2$. It can then be checked that

$$g \circ h = g \circ \phi \circ \iota_2 = \pi_2 \circ \iota_2 = \mathrm{id}_{M_3}.$$

■

21.2 Free Modules

Moral: A *free module* is a module with a basis.

Definition: A subset $X = \{x_i\}$ is *linearly independent* iff

$$\sum r_i x_i = 0 \implies r_i = 0 \ \forall i.$$

Definition: A subset X *spans* M iff

$$m \in M \implies m = \sum_{i=1}^{n} r_i x_i \quad \text{for some } r_i \in R,\ x_i \in X.$$

Definition: A subset X is a basis $\iff$ it is a linearly independent spanning set.

Example: $\mathbb{Z}_6$ is an abelian group and thus a $\mathbb{Z}$-module, but not free because $3 \curvearrowright [2] = [6] = 0$, so there are torsion elements. This contradicts linear independence for any subset.

Theorem (Characterization of Free Modules): Let R be a unital ring and M a unital R-module (so $1 \curvearrowright m = m$).

TFAE:

- There exists a nonempty basis of M.
- $M = \oplus_{i \in I} R$ for some index set I.
- There exists a non-empty set X and a map $\iota : X \hookrightarrow M$ such that given $f : X \to N$ for N any R- module, $\exists ! \tilde{f} : M \to N$ such that the following diagram commutes.

$$\begin{tikzcd}
M \arrow[dr, dotted, "\exists ! \tilde{f}"] & \\
X \arrow[u, hook, "\iota"] \arrow[r, "f"] & N
\end{tikzcd}$$

Definition: An R-module is *free* iff any of 1,2, or 3 hold.

Proof of $1 \implies 2$*:*

Let X be a basis for M, then define $M \to \oplus_{x \in X} Rx$ by $\phi(m) = \sum r_i x_i$.

It can be checked that

- This is an R-module homomorphism,
- $\phi(m) = 0 \implies r_j = 0\ \forall j \implies m = 0$, so ϕ is injective,
- ϕ is surjective, since X is a spanning set.

So $M \cong \bigoplus_{x \in X} Rx$, so it only remains to show that $Rx \cong R$. We can define the map

$$\begin{aligned}
\pi_x : R &\to Rx \\
r &\mapsto rx.
\end{aligned}$$

Then π_x is onto, and is injective exactly because X is a linearly independent set. Thus $M \cong \oplus R$.

■

Proof of $1 \implies 3$*:*

Let X be a basis, and suppose there are two maps $X \xrightarrow{\iota} M$ and $X \xrightarrow{f} M$. Then define

$$\begin{aligned} \tilde{f} : M &\to N \\ \sum_i r_i x_i &\mapsto \sum_i r_i f(x_i). \end{aligned}$$

This is clearly an R-module homomorphism, and the diagram commutes because $(\tilde{f} \circ \iota)(x) = f(x)$. This is unique because $\tilde{f}$ is determined precisely by $f(X)$.

■

Proof of $3 \implies 2$*:*

We use the usual "2 diagram" trick to produce maps

$$\begin{aligned} \tilde{f} &: M \to \bigoplus_{x \in X} R \\ \tilde{g} &: \bigoplus_{x \in X} R \to M. \end{aligned}$$

Then commutativity forces

$$\tilde{f} \circ \tilde{g} = \tilde{g} \circ \tilde{f} = \mathrm{id}.$$

■

Proof of $2 \implies 1$*:*

We have $M = \oplus_{i \in I} R$ by (2). So there exists a map

$$\psi : \oplus_{i \in I} R \to M,$$

so let $X \coloneqq \left\{ \psi(1_i) \;\middle|\; i \in I \right\}$, which we claim is a basis.

To see that X is a basis, suppose $\sum r_i \psi(1_i) = 0$. Then $\psi(\sum r_i 1_i) = 0$ and thus $\sum r_i 1_i = 0$ and $r_i = 0$ for all i.

Checking that it's a spanning set: Exercise.

■

Corollary: Every R-module is the homomorphic image of a free module.

Proof: Let M be an R-module, and let X be any set of generators of R. Then we can make a map

$$M \to \bigoplus_{x \in X} R$$

and there is a map $X \hookrightarrow M$, so the universal property provides a map

$$\tilde{f} : \bigoplus_{x \in X} R \to M.$$

Moreover, $\bigoplus_{x \in X} R$ is free.

$\blacksquare$

Examples:

- $\mathbb{Z}_n$ is **not** a free $\mathbb{Z}$-module for any n.
- If V is a vector space over a field k, then V is a free k-module (even if V is infinite dimensional).
- Every nonzero submodule of a free module over a PID is free.

Some facts:

Let $R = k$ be a field (or potentially a division ring).

1. Every maximal linearly independent subset is a basis for V.
2. Every vector space has a basis.
3. Every linearly independent set is contained in a basis
4. Every spanning set contains a basis.
5. Any two bases of a vector space have the same cardinality.

Theorem (Invariant Dimension): Let R be a commutative ring and M a free R-module.

If X_1, X_2 are bases for R, then $|X_1| = |X_2|$.

Any ring satisfying this condition is said to have the **invariant dimension property**.

> Note that it's difficult to say much more about generic modules. For example, even a finitely generated module may *not* have an invariant number of generators.

22 Tuesday November 5th

22.1 Free vs Projective Modules

Let R be a PID. Then any nonzero submodule of a free module over a PID is free, and any projective module over R is free.

Recall that a module M is **projective** $\iff$ M is a direct summand of a free module.

In general,

- Free $\implies$ projective, but
- Projective $\not\Longrightarrow$ free.

Example:

Consider $\mathbb{Z}_6 = \mathbb{Z}_2 \oplus \mathbb{Z}_3$ as a $\mathbb{Z}$-module. Is this free as a $\mathbb{Z}$-module?

Note that $\mathbb{Z}_2$ is a submodule and thus projective, but $\mathbb{Z}_2$ is not free since it is not a free module over $\mathbb{Z}$. What fails here is that $\mathbb{Z}_6$ is not a PID, since it is not a domain.

22.2 Annihilators

Definition: Let $m \in M$ a module, then define

$$\mathrm{Ann}_m := \left\{ r \in R \;\middle|\; r.m = 0 \right\} \trianglelefteq R.$$

We can then define a map

$$\begin{aligned} \phi : R &\to R.m \\ r &\mapsto r.m. \end{aligned}$$

Then $\ker \phi = \mathrm{Ann}_m$, and $R/\mathrm{Ann} \cong R.m$.

We can also define

$$M_t := \left\{ m \in M \;\middle|\; \mathrm{Ann}_m \neq 0 \right\} \leq M.$$

Lemma: Let R be a PID and p a prime element. Then

- If $p^i m = 0$ then $\mathrm{Ann}_m = (p^j)$ where $0 \leq j \leq i$.
- If $\mathrm{Ann}_m = (p^i)$, then $p^j m \neq 0$ for any $j < m$.

Proof of (1): Since we are in a PID and the annihilator is an ideal, we have $\mathrm{Ann}_m := (r)$ for some $r \in M$. Then $p^i \in (r)$, so $r \;\middle|\; p^i$. But p was prime, to up to scaling by units, we have $r = p^j$ for some $j \leq i$.

■

Proof of (2): Towards a contradiction, suppose that $\mathrm{Ann}_m = (p^i)$ and $p^j m = 0$ for some $j < i$. Then $p^j \in \mathrm{Ann}_m$, so $p^j \;\middle|\; p^i$. But this forces $j \leq i$, a contradiction.

■

Some terminology:

- Ann_m is the **order ideal** of m.
- M_t is the **torsion submodule** of M.
- M is **torsion** iff $M = M_t$.
- M is **torsion free** iff $M_t = 0$.
- $\mathrm{Ann}_m = (r)$ is said to have **order** r.
- Rm is the **cyclic module** generated by m.

Theorem: A finitely generated *torsion-free* module over a PID is free.

Proof: Let $M = \langle X \rangle$ for some finite generating set.

We can assume $M \neq (0)$. If $m \neq 0 \in M$, with $rm = 0$ iff $r = 0$.

So choose $S = \{x_1, \cdots, x_n\} \subseteq X$ to be a maximal linearly independent subset of generators, so

$$\sum r_i x_i = 0 \implies r_i = 0 \ \forall i.$$

Consider the submodule $F := \langle x_1, \cdots, x_n \rangle \leq M$; then S is a basis for F and thus F is free.

The claim is that $M \cong F$. Supposing otherwise, let $y \in X \setminus S$. Then $S \bigcup \{y\}$ can not be linearly independent, so there exists $r_y, r_i \in R$ such that

$$r_y y + \sum r_i x^i = 0.$$

Thus $r_y y = -\sum r_i x^i$, where $r_y \neq 0$.

Since $|X| < \infty$, let

$$r = \prod_{y \in X \setminus S} r_y.$$

Then $rX = \left\{ rx \;\middle|\; x \in X \right\} \subseteq F$, and $rM \leq F$.

Now using the particular r we've just defined, define a map

$$\begin{aligned} f : M &\to M \\ m &\mapsto rm. \end{aligned}$$

Then $\operatorname{im} f = r.M$, and since M is torsion-free, $\ker f = (0)$. So $M \cong rM \subseteq F$ and M is free.

■

Theorem: Let M be a finitely generated module over a PID R. Then M can be decomposed as

$$M \cong M_t \oplus F$$

where M_t is torsion and F is free of finite rank, and $F \cong M/M_t$.

Note: we also have $M/F \cong F_t$ since this is a direct sum.

Proof:

Part 1: M/M_t is torsion free.

Suppose that $r(m + M_t) = M_t$, so that r acting on a coset is the zero coset. Then $rm + M_t = M_t$, so $rm \in M_t$, so there exists some r' such that $r'(rm) = 0$ by definition of M_t. But then $(r'r)m = 0$, so in fact $m \in M_t$ and thus $m + M_t = M_t$, making M/M_t torsion free.

Part 2: $F \cong M/M_t$.

We thus have a SES

$$0 \to M_t \to M \to M/M_t := F \to 0,$$

and since we've shown that F is torsion-free, by the previous theorem F is free. Moreover, every SES with a free module in the right-hand slot splits:

$$\begin{tikzcd}
 & & & X \arrow[dl, tail, "f"'] \arrow[d, hook, "\iota"] & \\
0 \arrow[r] & M_t \arrow[r] & M \arrow[r, "f"'] & F \arrow[r] \arrow[l, dotted, bend right, "h"'] & 0
\end{tikzcd}$$

For $X = \{x_j\}$ a generating set of F, we can choose elements $\{y_i\} \in \pi^{-1}(\iota(X))$ to construct a set map $f : X \to M$. By the universal property of free modules, we get a map $h : F \to M$.

It remains to check that this is actually a splitting, but we have

$$\pi \circ h(x_j) = \pi(h(\iota(x_j))) = \pi(f(x_j)) = \pi(y_j) = x_j.$$

Lemma: Let R be a PID, and $r \in R$ factor as $r = \prod p_i^{k_i}$ as a prime factorization. Then

$$R/(r) \cong \bigoplus R/(p_i^{k_i}).$$

Since R is a UFD, suppose that $\gcd(s,t) = 1$. Then the claim is that

$$R/(st) = R/(s) \oplus R/(t),$$

which will prove the lemma by induction.

Define a map

$$\begin{aligned}
\alpha : R/(s) \oplus R/(t) &\to R/(st) \\
(x + (s), y + (t)) &\mapsto tx + sy + (st).
\end{aligned}$$

Exercise: Show that this map is well-defined.

Since $\gcd(s,t) = 1$, there exist u, v such that $su + vt = 1$. Then for any $r \in R$, we have

$$rsu + rvt = r,$$

so for any given $r \in R$ we can pick $x = tv$ and $y = su$ so that this holds. As a result, the map α is onto.

Now suppose $tx + sy \in (st)$; then $tx + sy = stz$. We have $su + vt = 1$, and thus

$$utx + usy = ustz \implies utx + (y - tvy) = ustz.$$

We can thus write

$$y = ustv - utx + tvy \in (t).$$

Similarly, $x \in (t)$, so $\ker \alpha = 0$.

■

22.3 Classification of Finitely Generated Modules Over a PID

Theorem (Classification of Finitely Generated Modules over a PID):

Let M be a finitely generated R-module where R is a PID. Then

1. $$M \cong F \bigoplus_{i=1}^{t} R/(r_i)$$

   where F is free of finite rank and $r_1 \Big| r_2 \Big| \cdots \Big| r_t$. The rank and list of ideals occurring is uniquely determined by M. The r_i are referred to as the **invariant factors**.

b. $$M \cong F \bigoplus_{i=1}^{k} R/(p_i^{s_i})$$

   where F is free of finite rank and p_i are primes that need not be distinct. The rank and ideals are uniquely determined by M. The $p_i^{s_i}$ are referred to as **elementary divisors**.

23 Thursday November 7th

23.1 Projective Modules

Definition: A **projective** module P over a ring R is an R-module such that the following diagram commutes:

$$\begin{tikzcd} & P \arrow[dl, dashed, "\exists\phi"'] \arrow[d, "f"] \\ M \arrow[r, "g"] & N \end{tikzcd}$$

i.e. for every surjective map $g : M \twoheadrightarrow N$ and every map $f : P \to N$ there exists a lift $\phi : P \to M$ such that that $g \circ \phi = f$.

Theorem: Every free module is projective.

Proof: Suppose $M \twoheadrightarrow N \to 0$ and $F \xrightarrow{f} N$, so we have the following situation:

$$\begin{tikzcd} & x \arrow[d, hook] \arrow[ddl, dotted] & \\ & F \arrow[dl, dashed, "\exists\phi"'] \arrow[d, "f"] & \\ M \arrow[r, two heads, "g"] & N \arrow[r, dotted] & 0 \end{tikzcd}$$

For every $x \in X$, there exists an $m_x \in M$ such that $g(m_x) = f(i(x))$. By freeness, there exists a $\phi : F \to M$ such that this diagram commutes.

$\blacksquare$

Corollary: Every R-module is the homomorphic image of a projective module.

Proof: If M is an R-module, then $F \twoheadrightarrow M$ where F is free, but free modules are surjective.

$\blacksquare$

Theorem: Let P be an R-module. Then TFAE:

a. P is projective.

b. Every SES $0 \to M \to N \to P \to 0$ splits.

c. There exists a free module F such that $F = P \oplus K$ for some other module K.

Proof:

$a \implies b$:

We set up the following situation, where s is produced by the universal property:

$$\begin{tikzcd}
 & & & P \arrow[dl, "\exists s"'] \arrow[d, hook, "\mathrm{id}"] & \\
0 \arrow[r] & M \arrow[r] & N \arrow[r, two heads] & P \arrow[r] & 0
\end{tikzcd}$$

$\blacksquare$

$b \implies c$:

Suppose we have $0 \to M \to N \to P \to 0$ a SES which splits, then $N \cong M \oplus P$ by a previous theorem.

$\blacksquare$

$c \implies a$:

We have the following situation:

$$\begin{tikzcd}
 & F = P \oplus K \arrow[d, bend right, "\pi"'] \arrow[ddl, dotted, "\exists h"'] \\
 & P \arrow[u, bend right, "\iota"'] \arrow[dl, dotted, "\phi = \iota \circ h"] \arrow[d, "f"] \\
M \arrow[r, two heads] & N
\end{tikzcd}$$

By the previous argument, there exists an $h : F \to M$ such that $g \circ h = f \circ \pi$. Set $\phi = h \circ \iota$.

Exercise: Check that $g \circ \phi = f$.

$\blacksquare$

Theorem: $\bigoplus P_i$ is projective $\iff$ each P_i is projective.

Proof:

$\implies$: Suppose $\oplus P_i$ is projective.

Then there exists some $F = K \oplus \bigoplus P_i$ where F is free. But then P_i is a direct summand of F, and is thus projective.

$\impliedby$: Suppose each P_i is projective.

Then there exists $F_i = P_i \oplus K_i$, so $F := \bigoplus F_i = \bigoplus (P_i \oplus K_i) = \bigoplus P_i \oplus \bigoplus K_i$. So $\bigoplus P_i$ is a direct summand of a free module, and thus projective.

■

Note that a direct sum has *finitely many* nonzero terms. Can use the fact that a direct sum of free modules is still free by taking a union of bases.

Example of a projective module that is not free:

Take $R = \mathbb{Z}_6$, which is not a PID and not a domain. Then $\mathbb{Z}_6 = \mathbb{Z}_2 \oplus \mathbb{Z}_3$, and $\mathbb{Z}_2, \mathbb{Z}_3$ are projective R-modules. By previous statements, we know these are torsion as $\mathbb{Z}$-modules, and thus not free.

23.2 Endomorphisms as Matrices

See section 7.1 in Hungerford

Let $M_{m,n}(\mathbb{R})$ denote $m \times n$ matrices with coefficients in R. This is an R-R bimodule, and since R is not necessarily a commutative ring, these two module actions may not be equivalent.

If $m = n$, then $M_{n,n}(R)$ is a ring under the usual notions of matrix addition and multiplication.

Theorem: Let V, W be vector spaces where $\dim V = m$ and $\dim W = n$. Let $\hom_k(V, W)$ be the set of linear transformations between them.

Then $\hom_k(V, W) \cong M_{m,n}(k)$ as k-vector spaces.

Proof: Choose bases of V, W. Then consider

$$\begin{aligned} T : V &\to W \\ v_1 &\mapsto \sum_{i=1}^{n} a_{1,i}\ w_i \\ v_2 &\mapsto \sum_{i=1}^{n} a_{2,i}\ w_i \\ &\vdots \end{aligned}$$

This produces a map

$$\begin{aligned} f : \hom_k(V, W) &\to M_{m,n}(k) \\ T &\mapsto (a_{i,j}), \end{aligned}$$

which is a matrix.

Exercise: Check that this is bijective.

$\blacksquare$

Theorem: Let M, N be free left R-modules of rank m, n respectively. Then $\hom_R(M, N) \cong M_{m,n}(R)$ as R-R bimodules.

Notation: Suppose M, N are free R-modules, then denote β_m, β_n be fixed respective bases. We then write $[T]_{\beta_m,\beta_n} := (a_{i,j})$ to be its *matrix representation.*

Theorem: Let R be a ring and let V, W, Z be three free left R-modules with bases $\beta_v, \beta_w, \beta_z$ respectively. If $T : V \to W, S : W \to Z$ are R-module homomorphisms, then $S \circ T : V \to Z$ exists and

$$[S \circ T]_{\beta_v,\beta_z} = [T]_{\beta_v,\beta_w}[S]_{\beta_w,\beta_z}$$

Proof: Exercise.

Show that

$$(S \circ T)(v_i) = \sum_j^t \sum_k^m a_{ik} b_{kj} z_j.$$

$\blacksquare$

23.3 Matrices and Opposite Rings

Suppose $\Gamma : \hom_R(V, V) \to M_n(R)$ and V is a free left R-module. By the theorem, we have $\Gamma(T \circ S) = \Gamma(S)\Gamma(T)$. We say that Γ is an **anti-homomorphism**.

To address this mixup, given a ring R we can define R^{op} which has the same underlying set of R but with the modified multiplication

$$x \cdot y := yx \in R.$$

If R is commutative, then $R \cong R^{op}$.

$\blacksquare$

Theorem: Let R be a unital ring and V an R-module.

Then $\hom_R(V, V) \cong M_n(R^{op})$ as rings.

Proof: Since $\Gamma(S \circ T) = \Gamma(T)\Gamma(S)$, define a map

$$\begin{aligned} \Theta : M_{n,n}(R) &\to M_{n,n}(R^{op}) \\ A &\mapsto A^t. \end{aligned}$$

Then

$$\Theta(AB) = (AB)^t = B^t A^t = \Theta(B)\Theta(A),$$

so Θ is an anti-isomorphism.

Thus $\Theta \circ \Gamma$ is an anti-anti-homomorphism, i.e. a usual homomorphism.

■

Definition: A matrix A is **invertible** iff there exists a B such that $AB = BA = \mathrm{id}_n$.

Proposition: Let R be a unital ring and V, W free R-modules with $\dim V = n, \dim W = m$. Then

1. $T \in \hom_R(V, W)$ is an isomorphisms iff $[T]_{\beta_v,\beta_w}$ is invertible.
2. $[T^{-1}]_{\beta_v,\beta_w} = [T]_{\beta_v,\beta_w}^{-1}$.

Definition: We'll say that two matrices A, B are **equivalent** iff there exist P, Q invertible such that $PAQ = B$.

24 Tuesday November 12th

24.1 Equivalence and Similarity

Recall from last time:

If V, W are free left R-modules of ranks m, n respectively with bases β_v, β_w respectively, then

$$\hom_R(V, W) \cong M_{m,n}(R).$$

Definition: Two matrices $A, B \in M_{m\times n}(R)$ are **equivalent** iff

$$\exists P \in \mathrm{GL}(m, R),\ \exists Q \in \mathrm{GL}(n, R) \quad \text{such that} \quad A = PBQ.$$

Definition: Two matrices $A, B \in M_m(R)$ are **similar** iff

$$\exists P \in \mathrm{GL}(m, R) \quad \text{such that} \quad A = P^{-1}BP.$$

Theorem: Let $T : V \to W$ be an R-module homomorphism.

Then T has an $m \times n$ matrix relative to other bases for $V, W \iff$

$$B = P[T]_{\beta_v,\beta_w}Q.$$

Proof: $\implies$:

Let β_v', β_w' be other bases. Then we want $B = [T]_{\beta_v',\beta_w'}$, so just let

$$P = [\mathrm{id}]_{\beta_v',\beta_v} \quad Q = [\mathrm{id}]_{\beta_w,\beta_w'}.$$

■

$\impliedby$:

Suppose $B = P[T]_{\beta_v,\beta_w}Q$ for some P, Q.

Let $g : V \to V$ be the transformation associated to P, and $h : W \to W$ associated to Q^{-1}.

Then

$$
\begin{aligned}
P &= [\mathrm{id}]_{g(\beta_v),\beta_v} \\
\implies Q^{-1} &= [\mathrm{id}]_{h(\beta_w),\beta_w} \\
\implies Q &= [\mathrm{id}]_{\beta_w,h(\beta_w)} \\
\implies B &= [T]_{g(\beta_v),h(\beta_w)}.
\end{aligned}
$$

■

Corollary: Let V be a free R-module and β_v a basis of size n.

Then $T : V \to V$ has an $n \times n$ matrix relative to β_v relative to another basis $\iff$

$$B = P[T]_{\beta_v,\beta_v} P^{-1}.$$

> Note how this specializes to the case of linear transformations, particularly when B is diagonalizable.

24.2 Review of Linear Algebra:

Let D be a division ring. Recall the notions of rank and nullity, and the statement of the rank-nullity theorem.

Note that we can always factor a linear transformation $\phi : E \to F$ as the following short exact sequence:

$$0 \to \ker \phi \to E \xrightarrow{\phi} \text{im } \phi \to 0,$$

and since every module over a division ring is free, this sequence splits and $E \cong \ker \phi \oplus \text{im } \phi$. Taking dimensions yields the rank-nullity theorem.

Let $A \in M_{m,n}(D)$ and define

- $R(A) \in D^n$ is the span of the rows of A, and
- $C(A) \in D^m$ is the span of the columns of A.

Recall that finding a basis of the **row space** involves doing Gaussian Elimination and taking the rows which have nonzero pivots.

For a basis of the **column space**, you take the corresponding columns in the *original* matrix.

> Note that in this case, $\dim R(A) = \dim C(A)$, and in fact these are always equal.

Theorem (Rank and Equivalence): Let $\phi : V \to W$ be a linear transformation and A be the matrix of ϕ relative to β_v, β_v'.

Then $\dim \text{im } \pi = \dim C(A) = \dim R(A)$.

Proof: Construct the matrix $A = [\phi]_{\beta_v,\beta_w}$.

Then $\phi : V \to W$ descends to a map $A : D^m \to D^n$. Writing the matrix A out and letting $v \in D^m$ a row vector act on A from the *left* yields a column vector $Av \in D^n$.

But then im ϕ corresponds to $R(A)$, and so

$$\dim \operatorname{im} \phi = \dim R(A) = \dim C(A).$$

$\blacksquare$

24.3 Canonical Forms

Let $1 \leq r \leq \min(m, n)$, and define E_r to be the $m \times n$ matrix with the $r \times r$ identity matrix in the top-left block.

Theorem: Let $A, B \in M_{m,n}(D)$. Then

1. A is equivalent to $E_r \iff \operatorname{rank} A = r$
    - That is, $\exists P, Q$ such that $E_r = PAQ$
2. A is equivalent to B iff $\operatorname{rank} A = \operatorname{rank} B$.
3. E_r for $r = 0, 1, \cdots, \min(m, n)$ is a complete set of representatives for the relation of matrix equivalence on $M_{m,n}(D)$.

Let $X = M_{m,n}(D)$ and $G = \mathrm{GL}_m(D) \times \mathrm{GL}_n(D)$, then

$$G \curvearrowright X \text{ by } (P, Q) \curvearrowright A := PAQ^{-1}.$$

Then the orbits under this action are exactly $\left\{ E_r \;\middle|\; 0 \leq r \leq \min(m, n) \right\}$.

Proof: Note that 2 and 3 follow from 1, so we'll show 1.

$\implies$:

Let A be an $m \times n$ matrix for some linear transformation $\phi : D^m \to D^n$ relative to some basis. Assume $\operatorname{rank} A = \dim \operatorname{im} \phi = r$. We can find a basis such that $\phi(u_i) = v_i$ for $1 \leq i \leq r$, and $\phi(u_i) = 0$ otherwise. Relative to this basis, $[\phi] = E_r$. But then A is equivalent to E_r.

$\impliedby$:

If $A = PE_rQ$ with P, Q invertible, then $\dim \operatorname{im} A = \dim \operatorname{im} E_r$, and thus $\operatorname{rank} A = \operatorname{rank} E_r = r$.

How do we do this? Recall the row operations:

- Interchange rows
- Multiply a row by a unit
- Add one row to another

But each corresponds to left-multiplication by an elementary matrix, each of which is invertible. If you proceed this way until the matrix is in RREF, you produce $P \prod P_i A$. You can now multiply on the *right* by elementary matrices to do column operations and move all pivots to the top-left block, which yields E_r.

$\blacksquare$

Theorem: Let $A \in M_{m,n}(R)$ where R is a PID.

Then A is equivalent to a matrix with L_r in the top-left block, where L_r is a diagonal matrix with $L_{ii} = d_i$ such that $d_1 \mid d_2 \mid \cdots \mid d_r$. Each (d_i) is uniquely determined by A.

25 Thursday November 14th

25.1 Equivalence to Canonical Forms

Let D be a division ring and k a field.

Recall that a matrix A is *equivalent* to $B \iff \exists P, Q$ such that $PBQ = A$. From a previous theorem, if $\operatorname{rank}(A) = r$, then A is equivalent to a matrix with I_r in the top-left block.

Theorem: Let A be a matrix over a PID R. Then A is equivalent to a matrix with L_r in the top-left corner, where $L_r = \operatorname{diag}(d_1, d_2, \cdots, d_r)$ and $d_1 \mid d_2 \mid \cdots \mid d_r$, and the d_i are uniquely determined.

Theorem: Let A be an $n \times n$ matrix over a division ring D. TFAE:

1. $\operatorname{rank} A = n$.
2. A is equivalent to I_n.
3. A is invertible.

$1 \implies 2$: Use Gaussian elimination.

$2 \implies 3$: $A = PI_nQ = PQ$ where P, Q are invertible, so $PQ = A$ is invertible.

$3 \implies 1$: If A is invertible, then $A : D^n \to D^n$ is bijective and thus surjective, so $\dim \operatorname{im} A = n$.

Note: the image is now *row space* because we are taking *left* actions.

■

25.2 Determinants

Definition: Let $M_1, \cdots, M_n$ be R-modules, and then $f : \prod M_i \to R$ is n-linear iff

$$f(m_1, m_2, \cdots, rm_k + sm_k', \cdots, m_n) = rf(m_1, \cdots, m_k, \cdots m_k) + sf(m_1, \cdots, m_k', \cdots, m_n).$$

Example: The inner product is a 2-linear form.

Definition: f is **symmetric** iff

$$f(m_1, \cdots, m_n) = f(m_{\sigma(1)}, \cdots, m_{\sigma(n)}) \ \forall \sigma \in S_n.$$

Definition: f is **skew-symmetric** iff

$$f(m_1, \cdots, m_n) = \operatorname{sgn}(\sigma) f(m_{\sigma(1)}, \cdots, m_{\sigma(n)}) \ \forall \sigma \in S_n,$$

where

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \sigma \text{ is even} \\ -1 & \sigma \text{ is odd} \end{cases}.$$

Definition: f is **alternating** iff

$$m_i = m_j \text{ for some pair } (i,j) \implies f(m_1, \cdots, m_n) = 0.$$

Theorem: Let f be an n-linear form. If f is alternating, then f is skew-symmetric.

Proof: It suffices to show the $n = 2$ case. We have

$$\begin{aligned} 0 &= f(m + 1 + m_2, m_1 + m_2) \\ &= f(m_1, m_1) + f(m_1, m_2) + f(m_2, m_1) + f(m_2, m_2) \\ &= f(m_1, m_2) + f(m_2, m_1) \\ &\implies f(m_1, m_2) = -f(m_2, m_1). \end{aligned}$$

■

Theorem: Let R be a unital commutative ring and let $r \in R$ be arbitrary.

Then

$$\exists! f : \bigoplus_{i=1}^{n} R^n \to R,$$

where f is an alternating R-form such that $f(\mathbf{e}_i) = r$ for all i, where $\mathbf{e}_i = [0, 0, \cdots, 0, 1, 0, \cdots, 0, 0]$.

R^n is a free module, so f can be identified with a matrix once a basis is chosen.

Proof:

Existence: Let $x_i = [a_{i1}, a_{i2}, \cdots, a_{in}]$ and define

$$f(x_1, \cdots, x_n) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) r \prod_i a_{i\sigma(i)}.$$

Exercise: Check that $f(\mathbf{e}_1, \cdots, \mathbf{e}_n) = r$ and f is n-linear.

Moreover, f is alternating. Consider $f(x_1, \cdots, x_n)$ where $x_i = x_j$ for some $i \neq j$.

Letting $\phi = (i, j)$, we can write $S_n = A_n \coprod A_n \rho$.

If σ is even, then the summand is

$$(+1) r a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

Since $x_i = x_j$, we'll have $\prod_k a_{ik} = \prod a_{jk}$. Then consider applying $\sigma\rho$. We have

$$\begin{aligned} -r \prod a_{i\sigma(i)} &= -r a_{1\sigma(1)} \cdots \mathbf{a}_{j\sigma(j)} \cdots \mathbf{a}_{i\sigma(i)} \cdots a_{n,\sigma(n)} \\ = -r \prod a_{i\sigma(i)} &= -r a_{1\sigma(1)} \cdots \mathbf{a}_{i\sigma(i)} \cdots \mathbf{a}_{j\sigma(j)} \cdots a_{n,\sigma(n)}, \end{aligned}$$

which permutes the i, j terms. So these two terms cancel, the remaining terms are untouched.

Uniqueness: Let $x_i = \sum_j a_{ij}\mathbf{e}_j$. Then

$$\begin{aligned} f(x_1, \cdots, x_n) &= f(\sum_{j_1} a_j^1 \mathbf{e}_j, \cdots, \sum_{j_n} a_j^n \mathbf{e}_j) \\ &= \sum_{j_1} \cdots \sum_{j_n} f(\mathbf{e}_{j_1}, \cdots, \mathbf{e}_{j_n}) a_{1,j_1} \cdots a_{n,j_n} \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) f(\mathbf{e}_1, \cdots, \mathbf{e}_n) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) r a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}. \end{aligned}$$

■

Definition: Let R be a commutative unital ring and define $\det : M_n(R) \to R$ is the unique n-alternating form with $\det(I) = 1$, and is called the *determinant*.

Theorem: Let $A, B \in M_n(R)$. Then

a. $|AB| = |A||B|$

b. A is invertible $\iff |A| \in R^\times$

c. $A \sim B \implies |A| = |B|$.

d. $\left|A^t\right| = |A|$.

e. If A is triangular, then $|A|$ is the product of the diagonal entries.

Proof of a: Let B be fixed.

Let $\Delta_B : M_n(R) \to R$ be defined as $C \mapsto |CB|$. Then this is an alternating form, so by the theorem, $\Delta_B = r\det$. But then $\Delta_B(C) = r|C|$, so $r|C| = |CB|$. So pick $C = I$, then $r = |B|$.

■

Proof of b: Suppose A is invertible.

Then $AA^{-1} = I$, so $\left|AA^{-1}\right| = |A|\left|A^{-1}\right| = 1$, which shows that $|A|$ is a unit.

■

Proof of c: Let $A = PBP^{-1}$. Then

$$|A| = \left|PBP^{-1}\right| = |P||B|\left|P^{-1}\right| = |P|\left|P^{-1}\right||B| = |B|.$$

■

Proof of d: Let $A = (a_{ij})$, so $B = (b_{ij}) = (a_{ji})$. Then

$$\begin{aligned}
\left|A^t\right| &= \sum_{\sigma} \operatorname{sgn}(\sigma) \prod_k b_{k\sigma(k)} \\
&= \sum_{\sigma} \operatorname{sgn}(\sigma) \prod_k a_{\sigma(k)k} \\
&= \sum_{\sigma^{-1}} \operatorname{sgn}(\sigma) \prod_k a_{k\sigma^{-1}(k)} \\
&= \sum_{\sigma} \operatorname{sgn}(\sigma) \prod_k a_{k\sigma(k)} \\
&= |A|.
\end{aligned}$$

■

Proof of e: Let A be upper-triangular. Then

$$|A| = \sum_{\sigma} \operatorname{sgn}(\sigma) \prod_k a_{k\sigma(k)} = a_{11}a_{22}\cdots a_{nn}.$$

■

Next time:

- Calculate determinants
  - Gaussian elimination
  - Cofactors
- Formulas for A^{-1}
- Cramer's rule

26 Tuesday November 19th

26.1 Determinants

Let $A \in M_n(R)$, where R is a commutative unital ring.

Given $A = (a_{ij})$, recall that

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod a_{i,\sigma(i)}.$$

This satisfies a number of properties:

- $\det(AB) = \det A \det B$
- A invertible $\implies$ $\det A$ is a unit in R
- $A \sim B \implies \det(A) = \det(B)$
- $\det A^t = \det A$
- A is triangular $\implies$ $\det A = \prod a_{ii}$.

26.1.1 Calculating Determinants

1. **Gaussian Elimination**

   a. B is obtained from A by interchanging rows: $\det B = -\det A$

   b. B is obtained from A by multiplying $\det B = r \det A$

   c. B is obtained from A by adding a scalar multiple of one row to another: $\det B = \det A$.

2. **Cofactors** Let A_{ij} be the $(n-1) \times (n-1)$ minor obtained by deleting row i and column j, and $C_{ij} = (-1)^{i+j} \det A_{ij}$.

   Then **(theorem)** $\det A = \displaystyle\sum_{j=1}^{n} a_{ij} C_{ij}$ by expanding along either a row or column.

Theorem:

$$A \mathrm{Adj}(A) = \det(A) I_n,$$

where $\mathrm{Adj} = (C_{ij})^t$.

If A^{-1} is a unit, then $A^{-1} = \mathrm{Adj}(A)/\det(A)$.

26.1.2 Decomposition of a Linear Transformation:

Let $\phi : V \to V$ be a linear transformation of vector spaces. and $R = \hom_k(V, V)$. Then R is a ring.

Let $f(x) = \sum a_j x^j \in k[x]$ be an arbitrary polynomial. Then for $\phi \in R$, it makes sense to evaluate $f(\phi)$ where ϕ^n denotes an n-fold composition, and $f(\phi) : V \to V$.

Lemma:

- There exists a unique monic polynomial $q_\phi(x) \in k[x]$ such that $q_\phi(\phi) = 0$ and $f(\phi) = 0 \implies q_\phi \mathrel{\Big|} f$. q_ϕ is referred to as the **minimal polynomial** of ϕ.
- The exact same conclusion holds with ϕ replaced by a matrix A, yielding q_A.
- If A is the matrix of ϕ relative to a fixed basis, then $q_\phi = q_A$.

Proof of a and b: Fix ϕ, and define

$$\begin{aligned} \Gamma : k[x] &\to \hom_k(V, V) \\ f &\mapsto f(\phi). \end{aligned}$$

Since $\dim_k V^\vee = \dim_k V < \infty$ and $\dim_k k[x] = \infty$, we must have $\ker \Gamma \neq 0$.

Since $k[x]$ is a PID, we have $\ker \Gamma = (q)$ for some $q \in k[x]$. Then if $f(\phi) = 0$, we have $f(x) \in \ker \Gamma \implies q \mathrel{\Big|} f$. We can then rescale q to be monic, which makes it unique.

> Note: for (b), just replace ϕ with A everywhere.

$\blacksquare$

Proof of c: Suppose $A = [\phi]_{\mathcal{B}}$ for some fixed basis $\mathcal{B}$.

Then $\hom_k(V, V) \cong M_n(k)$, so we have the following commutative diagram:

$$\begin{tikzcd}
k[x] \arrow[r, "\Gamma_\phi"] \arrow[dr, "\Gamma_A"'] & \hom_k(V, V) \arrow[d, hook, two heads, "\cong"] \\
& M_n(k)
\end{tikzcd}$$

■

26.1.3 Finitely Generated Modules over a PID

Let M be a finitely generated module over R a PID. Then

$$\begin{aligned}
M &\cong F \oplus \bigoplus_{i=1}^{n} R/(r_i) \quad r_1 \,\Big|\, r_2 \,\Big|\, \cdots r_n \\
M &\cong F \oplus \bigoplus_{i=1}^{n} R/(p_i^{s_i}) \quad p_i \text{ not necessarily distinct primes. }.
\end{aligned}$$

Letting $R = k[x]$ and $\phi : V \to V$ with $\dim_k V < \infty$, V becomes a $k[x]$-module by defining

$$f(x) \curvearrowright \mathbf{v} \coloneqq f(\phi)(\mathbf{v})$$

Note that W is a $k[x]$-submodule iff $\phi : W \to W$.

Let $v \in V$, and $\langle v \rangle = \left\{ \phi^i(v) \,\middle|\, i = 0, 1, 2, \cdots \right\}$ is the **cyclic submodule generated by** v, and we write $\langle v \rangle = k[x].v$.

Theorem: Let $\phi : V \to V$ be a linear transformation. Then

1. There exist cyclic $k[x]$-submodules V_i such that $V = \bigoplus_{i=1}^{t} V_i$, where for each i there exists a $q_i : V_i \to V_i$ such that $q_1 \,\Big|\, q_2 \,\Big|\, \cdots \,\Big|\, q_t$.
2. There exist cyclic $k[x]$-submodules V_j such that $V = \bigoplus_{j=1}^{\nu}$ and $p_j^{m_j}$ is the minimal polynomial of $\phi : V_j \to V_j$.

Proof: Apply the classification theorem to write $V = \bigoplus R/(r_i)$ as an invariant factor decomposition.

Then $R/(q_i) \cong V_i$, some vector space, and since there is a direct sum decomposition, the invariant factors are minimal polynomials for $\phi_i : V_i \to V_i$, and thus $k[x]/(q_i)$.

■

26.1.4 Canonical Forms for Matrices

We'll look at

- Rational Canonical Form
- Jordan Canonical Form

Theorem: Let $\phi : V \to V$ be linear, then V is a cyclic $k[x]$-module and $\phi : V \to V$ has minimal polynomial $q(x) = \sum_j a_j x^j$ iff $\dim V = n$ and V has an ordered basis of the form

$$[\phi]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{bmatrix}$$

with ones on the super-diagonal.

Proof:

$\Longleftarrow$:

Let $V = k[x].v = \left\langle v, \phi(v), \cdots, \phi^{n-1}(v) \right\rangle$ where $\deg q(x) = n$. The claim is that this is a linearly independent spanning set.

Linear independence: suppose $\sum_{j=0}^{n-1} k_j \phi^j(v) = 0$ with some $k_j \neq 0$. Then $f(x) = \sum k_j x^j$ is a polynomial where $f(\phi) = 0$, but this contradicts the minimality of $q(x)$.

But then we have n linearly independent vectors in V which is dimension n, so this is a spanning set.

$\Longrightarrow$:

We can just check where basis elements are sent. Set $\mathcal{B} = \left\{ v, \phi(v), \cdots, \phi^{n-1}(v) \right\}$. Then

$$\begin{aligned} v &\mapsto \phi(v) \\ \phi(v) &\mapsto \phi^2(v) \\ &\vdots \\ \phi n - 1(v) &\mapsto \phi^n(v) = -\sum a_i \phi^i(v) \\ &. \end{aligned}$$

$\Longleftarrow$ Fix a basis $B = \{v_1, \cdots, v_n\}$ and $A = [\phi]_B$, then

$$\begin{aligned} v_1 &\mapsto v_2 = \phi(v_1) \\ v_1 &\mapsto v_3 = \phi^2(v_1) \\ v_{n-2} &\mapsto v_{n-1} = \phi^2(v_1). \end{aligned}$$

and

$$\phi^n(v) = -a_k v_1 \neq -a_1\phi(v_1), \cdots - a_{n-1}\phi^{n-1}(v_1).$$

Thus $V = k[x].v_1$, since $\dim V = n$ with $\left\{v_1, \phi(v_1), \cdots, \phi^{n-1}(v_1)\right\}$ as a basis.

$\blacksquare$

27 Thursday November 21

27.1 Cyclic Decomposition

Let $\phi : V \to V$ be a linear transformation; then V is a $k[x]$ module under $f(x) \curvearrowright v := f(\phi)(v)$.

By the structure theorem, since $k[x]$ is a PID, we have an invariant factor decomposition $V = \bigoplus V_i$ where each V_i is a cyclic $k[x]$-module. If q_i is the minimal polynomial for $\phi_i : V_i \to V_i$, then $q_i \mathrel{\Big|} q_{i+1}$ for all i.

We also have an elementary divisor decomposition where $p_i^{m_i}$ are the minimal polynomials for ϕ_i.

> Note: one is only for the restriction to the subspaces? Check.

Recall that if ϕ has minimal polynomial $q(x)$. Then if $\dim V = n$, there exists a basis of B if V such that $[\phi]_B$ is given by the **companion matrix** of $q(x)$. This is the **rational canonical form**.

Corollary: Let $\phi : V \to V$ be a linear transformation. Then V is a cyclic $k[x]$-module and ϕ has minimal polynomial $(x-b)^n \iff \dim V = n$ and there exists a basis such that

$$[\phi]_B = \begin{bmatrix} b & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & b & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & b & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & b & 1 \end{bmatrix}.$$

This is the **Jordan Canonical form**.

> Note that if k is not algebraically closed, we can only reduce to RCF. If k *is* closed, we can reduce to JCF, which is slightly nicer.

Proof:

Let $\delta = \phi - b \cdot \mathrm{id}_V$. Then

- $q(x)$ is the minimal polynomial for $\phi \iff x^n$ is the minimal polynomial for δ.
- A priori, V has two $k[x]$ structures – one given by ϕ, and one by δ.
- *Exercise*: V is cyclic with respect to the ϕ structure $\iff$ V is cyclic with respect to the the δ structure.

Then the matrix $[\delta]_B$ relative to an ordered basis for δ is with only zeros on the diagonal and 1s on the super-diagonal, and $[\phi]_B$ is the same but with b on the diagonal.

$\blacksquare$

Lemma: Let $\phi : V \to V$ with $V = \bigoplus_i^t V_i$ as $k[x]$-modules. Then M_i is a matrix of $\phi|_{V_i} : V_i \to V_i$ relative to some basis for $V_i \iff$ the matrix of ϕ wrt some ordered basis is given by

$$\begin{bmatrix} M_1 & & & \\ & M_2 & & \\ & & \ddots & \\ & & & M_t \end{bmatrix}.$$

Proof:

$\implies$: Suppose B_i is a basis for V_i and $[\phi]_{B_i} = M_i$. Then let $B = \bigcup_i B_i$; then B is a basis for V and the matrix is of the desired form.

$\impliedby$: Suppose that we have a basis B and $[\phi]_B$ is given by a block diagonal matrix filled with blocks M_i. Suppose $\dim M_i = n_i$. If $B = \{v_1, v_2, \cdots, v_n\}$, then take $B_1 = \{v_1, \cdots, v_{n_1}\}$ and so on. Then $[\phi_i]_{B_i} = M_i$ as desired.

■

Application: Let $V = \bigoplus V_i$ with q_i the minimal polynomials of $\phi : V_i \to V_i$ with $q_i \mid q_{i+1}$.

Then there exists a basis where $[\phi]_B$ is block diagonal with blocks M_i, where each M_i is in rational canonical form with minimal polynomial $q_i(x)$. If k is algebraically closed, we can obtain elementary divisors $p_i(x) = (x - b_i)^{m_i}$. Then there exists a similar basis where now each M_i is a *Jordan block* with b_i on the diagonals and ones on the super-diagonal.

Moreover, in each case, there is a basis such that $A = P[M_i]P^{-1}$ (where M_i are the block matrices obtained). When A is diagonalizable, P contains the eigenvectors of A.

Corollary: Two matrices are similar $\iff$ they have the same invariant factors and elementary divisors.

Example: Let $\phi : V \to V$ have invariant factors $q_1(x) = (x - 1)$ and $q_2(x) = (x - 1)(x - 2)$.

Then $\dim V = 3$, $V = V_1 \oplus V_2$ where $\dim V_1 = 1$ and $\dim V_2 = 2$. We thus have

$$[\phi]_B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -2 & 3 \end{pmatrix}.$$

Moreover, we have

$$V \cong \frac{k[x]}{(x-1)} \oplus \frac{k[x]}{(x-1)(x-2)} \cong \frac{k[x]}{(x-1)} \oplus \frac{k[x]}{(x-1)} \oplus \frac{k[x]}{(x-2)},$$

so the elementary divisors are $x - 1, x - 1, x - 2$.

> Invariant factor decompositions should correspond to rational canonical form blocks, and elementary divisors should correspond to Jordan blocks.

Theorem: Let A be an $n \times n$ matrix over k. Then the matrix $xI_n - A \in M_n(k[x])$ is equivalent in $k[x]$ to a diagonal matrix D with non-zero entries $f_1, f_2, \cdots f_t \in k[x]$ such that the f_i are monic and $f_i \mathrel{\Big|} f_{i+1}$. The non-constant polynomials among the f_i are the invariant factors of A.

Proof (Sketch): Let $V = k^n$ and $\phi : k^n \to k^n$ correspond to A under the fixed standard basis $\{e_i\}$. Then V has a $k[x]$-module structure induced by ϕ.

Let F be the free $k[x]$ module with basis $\{u_i\}_{i=1}^n$, and define the maps

$$\begin{aligned} \pi : F &\to k^n \\ u_i &\mapsto e_i \end{aligned}$$

and

$$\begin{aligned} \psi : F &\to F \\ u_i &\mapsto xu_i - \sum_j a_{ij} u_j. \end{aligned}$$

Then ψ relative to the basis $\{u_i\}$ is $xI_n - A$.

Then *(exercise)* the sequence

$$F \xrightarrow{\psi} F \xrightarrow{\pi} k^n \to 0$$

is exact, im $\pi = k^n$, and im $\psi = \ker \pi$.

We then have $k^n \cong F/\ker \pi = F/\text{im } \psi$, and since $k[x]$ is a PID,

$$xI_n - A \sim D := \begin{bmatrix} L_r & 0 \\ 0 & 0 \end{bmatrix}.$$

where L_r is diagonal with f_is where $f_i \mathrel{\Big|} f_{i+1}$.

However, $\det(xI_n - A) \neq 0$ because $xI_n - A$ is a monic polynomial of degree n.

But $\det xI_n - A = \det(D)$, so this means that L_r must take up the entire matrix of D, so there is no zero in the bottom-right corner. So $L_r = D$, and D is the matrix of ψ with respect to $B_1 = \{v_i\}$ and $B_2 = \{w_i\}$ with $\psi(v_i) = f_i w_i$.

Thus

$$\text{im } \psi = \bigoplus_{i=1}^n k[x] f_i w_i.$$

But then

$$V = k^n \cong F/\text{im }\psi \cong \frac{k[x]w_1 \oplus \cdots \oplus k[x]w_n}{k[x]f_1 w_1 \oplus \cdots \oplus k[x]f_n w_n}$$
$$\cong \bigoplus_{i=1}^{n} k[x]/(f_i).$$

■

28 Tuesday November 26th

28.1 Minimal and Characteristic Polynomials

Theorem

a. ? (Todo)

b. **(Cayley Hamilton)** If p is the minimal polynomial of a linear transformation ϕ, then $p(\phi) = 0$

c. For any $f(x) \in k[x]$ that is irreducible, $f(x) \mid p_\phi(x) \iff f(x) \mid q_\phi(x)$.

Proof of (a): ?

■

Proof of (b):

If $q_\phi(x) \mid p_\phi(x)$ and $q_\phi(\phi) = 0$, then $p_\phi(\phi) = 0$ as well.

■

Proof of (c): We have $f(x) \mid q_\phi(x) \implies f(x) \mid p_\phi(x)$ and $f(x) \mid p_\phi(x) \implies f(x) \mid q_i(x)$ for some i, and so $f(x) \mid q_\phi(x)$.

■

28.2 Eigenvalues and Eigenvectors

Definition: Let $\phi : V \to V$ be a linear transformation. Then

1. An **eigenvector** is a vector $\mathbf{v} = \mathbf{0}$ such that $\phi(\mathbf{v}) = \lambda\mathbf{v}$ for some $\lambda \in k$.
2. If such a $\mathbf{v}$ exists, then λ is called an **eigenvalue** of ϕ.

Theorem: The eigenvalues of ϕ are the roots of $p_\phi(x)$ in k.

Proof: Let $[\phi]_B = A$, then

$$
\begin{aligned}
&p_A(\lambda) = p_\phi(\lambda) = \det(\lambda I - A) = 0 \\
&\iff \exists \mathbf{v} \neq \mathbf{0} \text{ such that } (\lambda I - A)\mathbf{v} = \mathbf{0} \\
&\iff \lambda I \mathbf{v} = A\mathbf{v} \\
&\iff A\mathbf{v} = \lambda \mathbf{v} \\
&\iff \lambda \text{ is an eigenvalue and } \mathbf{v} \text{ is an eigenvector.}
\end{aligned}
$$

■

29 Tuesday December 3rd

29.1 Similarity and Diagonalizability

Recall that $A \sim B \iff A = PBP^{-1}$.

Fact: If $T : V \to V$ is a linear transformation and $\mathcal{B}, \mathcal{B}'$ are bases where $[T]_{\mathcal{B}} = A$ and $[T]_{\mathcal{B}'}$, then $A \sim B$.

Theorem: Let A be an $n \times n$ matrix. Then

1. A is similar to a diagonal matrix / diagonalizable $\iff$ A has n linearly independent eigenvectors.
2. $A = PDP^{-1}$ where D is diagonal and $P = [\mathbf{v_1}, \mathbf{v_2}, \cdots, \mathbf{v_n}]$ with the $\mathbf{v_i}$ linearly independent.

Proof: Consider $AP = PD$, then AP has columns $A\mathbf{v_i}$ and PD has columns $\lambda_i \mathbf{v_i}$. ■

Corollary: If A has distinct eigenvalues, then A is diagonalizable.

Examples:

1. Let

$$
A = \begin{bmatrix} 4 & 0 & 0 \\ -1 & 4 & 0 \\ 0 & 0 & 5 \end{bmatrix}
$$

   A has eigenvalues $4, 5$, and it turns out that A is defective.

   Note that $\dim \Lambda_4 + \dim \Lambda_5 = 2 < 3$, so the eigenvectors can't form a basis of $\mathbb{R}^3$.

2.

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

   A has eigenvalues $2, 8$. $\Lambda_2 = \text{span}_{\mathbb{R}} \left\{ [-1, 1, 0]^t, [-1, 0, 1]^t \right\}$ and $\Lambda_8 = \text{span}_{\mathbb{R}} \left\{ [1, 1, 1]^t \right\}$. These vectors become the columns of P, which is (by no coincidence!) an orthogonal matrix, since A was symmetric.

Exercise:

$$\begin{bmatrix} 0 & 4 & 2 \\ -1 & -4 & -1 \\ 0 & 0 & -2 \end{bmatrix}.$$

Find $J = JCF(A)$ (so $A = PJP^{-1}$) and compute P.

Definition: Let $A = (a_{ij})$, then define that *trace* of A by $\mathrm{Tr}(A) = \sum_i a_{ii}$.

The trace satisfies several properties:

- $\mathrm{Tr}(A + B) = \mathrm{Tr}(A) + \mathrm{Tr}(B)$,
- $\mathrm{Tr}(kA) = k\mathrm{Tr}(A)$,
- $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

Theorem: Let $T : V \to V$ be a linear transformation with $\dim V < \infty$, $A = [T]_{\mathcal{B}}$ with respect to some basis, and $p_T(x)$ be the characteristic polynomial of A.

Then

$$\begin{aligned} p_T(x) &= x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0, \\ c_0 &= (-1)^n \det(A), \\ c_{n-1} &= -\mathrm{Tr}(A). \end{aligned}$$

Proof: We have $p_T(0) = \det(0I_n - A) = \det(-A) = (-1)^n \det(A)$.

Compute $p_T(x)$ by expanding $\det xI - A$ along the first row. The first term looks like $\prod (x - a_{ii})$, and no other term contributes to the coefficient of x^{n-1}.

$\blacksquare$

Definition: A *Lie Algebra* is a vector space with an operation $[\,\cdot\,,\,\cdot\,] : V \times V \to V$ satisfying

1. Bilinearity,
2. $[x, x] = 0$,
3. The Jacobi identity $[x, [y, z]] = [y, [z, x]] + [z, [x, y]] = 0$.

Examples:

1. $L = \mathfrak{gl}(n, \mathbb{C}) = n \times n$ invertible matrices over $\mathbb{C}$ with $[A, B] = AB - BA$.
2. $L = \mathfrak{sl}(n, \mathbb{C}) = \left\{ A \in \mathfrak{gl}(n, \mathbb{C}) \;\middle|\; \mathrm{Tr}(A) = 0 \right\}$ with the same operation, and it can be checked that

$$\mathrm{Tr}([A, B]) = \mathrm{Tr}(AB - BA) = \mathrm{Tr}(AB) - \mathrm{Tr}(BA) = 0.$$

> This turns out to be a *simple* algebra, and simple algebras over $\mathbb{C}$ can be classified using root systems and Dynkin diagrams – this is given by type A_{n-1}.

30 Summary

- Groups and rings, including Sylow theorems,
- Classifying small groups,
- Finitely generated abelian groups,
- Jordan-Holder theorem,
- Solvable groups,
- Simplicity of the alternating group,
- Euclidean domains,
- Principal ideal domains,
- Unique factorization domains,
- Noetherian rings,
- Hilbert basis theorem,
- Zorn's lemma, and
- Existence of maximal ideals and vector space bases.

Previous course web pages:

- Fall 2017, Asilata Bapat