Algebra

D. Zack Garza

October 15, 2019

Contents

---

1 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

2 Major Theorems

Theorem 1 (Cauchy)**.** For any prime p dividing the order of G, there is an element x of order p (and thus a subgroup $H = \langle x \rangle$ of order p as well).

Theorem 2 (Lagrange)**.** If $H \leq G$ is a subgroup, then $|H| \,\Big|\, |G|$. Moreover,

$$|G| = [G : H]\ |H|.$$

Theorem 3 (Sylow 1)**.** If $|G| = n = \prod p_i^{a_i}$ as a prime factorization, then G has subgroups of order $p_i^{a_i}$ for every i and for every $1 \leq r \leq a_i$. In particular, $\mathrm{Syl}(p, G) \neq \emptyset$.

Moreover, every subgroup H of order p^k is normal in a subgroup of order p^{k+1} for $1 \leq k \leq \alpha_i$, and thus $H \leq P$ for some $P \in \mathrm{Syl}(p, G)$.

Theorem 4 (Sylow 2)**.** If $P_1, P_2 \in \mathrm{Syl}(p, G)$, then there exists a $g \in G$ such that $gP_1g = P_2$.

Theorem 5 (Sylow 3)**.** Let $|G| = p^n m$ and $r_p = |\mathrm{Syl}(p, G)|$. Then

- $r_p = 1 \mod p$,
- $r_p \,\Big|\, m$,
- $r_p = [G : N_G(P)]$.

Theorem 6 (Classification of finitely generated abelian groups)**.** If G is a finitely generated abelian group, then $G \cong F \oplus T$, where F is free abelian and T is a torsion group. If $|T| = n$, then $T \cong \bigoplus \mathbb{Z}_{p_i^{\alpha_i}}$ where $n = \prod p_i^{\alpha_i}$ is some factorization of n with the p_i **not necessarily distinct**.

Theorem 7. Conjugacy classes partition G

$$|G| = |Z(G)| + \sum_{\text{One representative in each orbit}} |C_G(g_i)| = \sum_{asdsa} [G : C(g_i)].$$

Theorem 8 (Orbit Stabilizer)**.** If $G \curvearrowright X$, then for any $x \in X$

$$[G : \mathrm{Stab}(x)] = |\mathcal{O}_x|, \quad \text{i.e.} \quad |G| = |\mathcal{O}_x||\mathrm{Stab}(x)|$$

where $\mathcal{O}_x = \{g \curvearrowright x \ni g \in G\} \subseteq X$ and $\mathrm{Stab}(x) = \{x \in X \ni \forall g \in G,\ g \curvearrowright x = x\} \leq G$.

Theorem 9 (Eisenstein's Criterion)**.** If $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$ and there exists a prime p such that

- p divides a_i for each $0 \leq i \leq n-1$,
- p does not divide a_n, and
- p^2 does not divide a_0,

Then f is irreducible over $\mathbb{Q}$.

Some nice lemmas:

- Every subgroup of a cyclic group is itself cyclic.
- $aH = bH \iff b^{-1}a \in H$.
- $A \leq G$ and $B \leq G \implies (A \bigcap B) \leq G$.
  - Corollary: $\#A = p, \#B = q \implies A \bigcap B = \{e\}$.
  - Corollary: $\#A = p, \#B = p \implies A = B$ or $A \bigcap B = \{e\}$.
- The Quaternion group has only one element of order 2, namely -1.
  - They also have the presentation $Q = \langle x, y, z \mid x^2 = y^2 = z^2 = xyz = -1\rangle$ or $Q = \langle x, y \mid x^4 = y^4 = e, x$
- A dihedral group always has presentation $D_n = \langle x, y \mid x^n = y^2 = (xy)^2 = e\rangle$, yielding at least 2 distinct elements of order 2.

3 Lecture 1 (Thu 15 Aug 2019)

We'll be using Hungerford's Algebra text.

3.1 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

3.2 Preliminaries

Definition 10. 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:

- Associativity: $(g_1 g_2)g_3 = g_1(g_2 g_3)$,
- Identity: $\exists e \in G \ni ge = eg = g$,
- Inverses: $g \in G \implies \exists h \in G \ni gh = gh = e$.

Example 11.

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

Definition 12. A subset $S \subseteq G$ is a **subgroup** of G iff

1. $s_1, s_2 \in S \implies s_1 s_2 \in S$
2. $e \in S$
3. $s \in S \implies s^{-1} \in S$

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 $\mathrm{SL}(n, \mathbb{R}) = \{A \in \mathrm{GL}(n, \mathbb{R}) \ni \det(A) = 1\}$

3.3 Cyclic Groups

Definition 13. A group G is **cyclic** iff G is generated by a single element.

Exercise 1. Show $\langle g \rangle = \{g^n \ni n \in \mathbb{Z}\} \cong \bigcap_{g \in G} \{H \ni H \leq G \text{ and } g \in H\}$.

Theorem 14. 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 15. Let $H \leq G$, and define a **right coset of** G by $aH = \{ah \ni H \in H\}$. A similar definition can be made for **left cosets**.

Then $aH = bH \iff b^{-1}a \in H$ 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 16 (Lagrange)**.** If G is a finite group and $H \leq G$, then $|H| \;\Big|\; |G|$.

Definition 17. 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

$$G/N = \{gN \ni g \in G\} \text{ where } (g_1 N)(g_2 N) = (g_1 g_2)N.$$

Given $H, K \leq G$, define $HK = \{hk \ni h \in H, k \in K\}$. We have a general formula,

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

3.4 Homomorphisms

Definition 18. Let G, G' be groups, then $\varphi : G \to G'$ is a **homomorphism** if $\varphi(ab) = \varphi(a)\varphi(b)$.

Example 19.
- $\exp : (\mathbb{R}, +) \to (\mathbb{R}^{>0}, \cdot)$ where $\exp(a+b) = e^{a+b} = e^a e^b = \exp(a)\exp(b)$.
- $\det : (\mathrm{GL}(n, \mathbb{R}), \times) \to (\mathbb{R}^\times, \times)$ where $\det(AB) = \det(A)\det(B)$.
- Let $N \trianglelefteq G$ and $\varphi G \to G/N$ given by $\varphi(g) = gN$.
- 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 20. 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.

3.5 Direct Products

Let G_1, G_2 be groups, then define

$$G_1 \times G_2 = \{(g_1, g_2) \ni g_1 \in G, g_2 \in G_2\} \text{ where } (g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2, h_2).$$

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

3.6 Finitely Generated Abelian Groups

Definition 21. 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 22. 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 23. 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 $r, s \in \mathbb{N}$ and p_i are (not necessarily distinct) primes.

Example 24. 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.

3.7 Fundamental Homomorphism Theorem

Let $\varphi : G \to G'$ be a group homomorphism and define $\ker \varphi = \{g \in G \ni \varphi(g) = e'\}$.

3.7.1 The First Homomorphism Theorem

Theorem 25. 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 2. Check that φ is well-defined.

3.7.2 The Second Theorem

Theorem 26. Let $K, N \leq G$ where $N \trianglelefteq G$. Then

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

Proof. Define a map $K \xrightarrow{\varphi} NK/N$ by $\varphi(k) = kN$. You can show that φ is onto, then look at $\ker\varphi$; note that $kN = \varphi(k) = N \iff k \in N$, and so $\ker\varphi = N \bigcap K$. $\square$

4 Lecture 2

Last time: 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

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

(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 $H \leq K$.

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. First make a map

$$\begin{aligned} G/K &\to G/H \\ \phi(gk) &= gH \end{aligned}$$

Exercise: Show that this map is onto, and that $\ker\phi \cong H/K$.

4.1 Permutation Groups

Let A be a set, then a *permutation* on A is a bijective map $A \circlearrowleft$. 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. Check 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 (see notes).

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

4.2 Orbits

Permutations S_A "acts" 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. Moreover, we have

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

and so every permutation is a product of transpositions. 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.

Define $A_n = \{\sigma \in S_n \ni \sigma \text{ is even}\}$. 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.

4.3 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*

$$G_x = \{g \in G \ni g \curvearrowright x = x\} \leq G$$

We can also look at the dual thing,

$$X_g = \{x \in X \ni g \curvearrowright x = x\}.$$

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

$$Gx = \{g \curvearrowright x \ni g \in G\}$$

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

$$|Gx| = [G : G_x] \tag{1}$$

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.

5 Lecture 3 (Aug 22)

Last time: 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

$$G_x = \{g \in G \ni g \curvearrowright x = x\} \leq G,$$

and the *orbit*

$$G.x = \mathcal{O}_x = \{g \curvearrowright x \ni x \in X\} \subseteq X.$$

When G is finite, we have

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

We can also consider the fixed points of X,

$$X_g = \{x \in X \ni g \curvearrowright x = x \forall g \in G\} \subseteq X$$

5.1 Burnside's Theorem

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

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

Proof:

Define $N = \{(g, x) \ni g \curvearrowright x = x\} \subseteq G \times X$, we then have

$$\begin{aligned} |N| &= \sum_{g \in G} |X_g| \\ &= \sum_{x \in X} |G_x| \\ &= \sum_{x \in X} \frac{|G|}{|G.x|} \\ &= |G| \left(\sum_{x \in X} \frac{1}{|Gx|} \right) \\ &= |G|v. \end{aligned}$$

Since the orbits partition X, say into $X = \bigcup_{i=1}^{v} \sigma_i$, let $\sigma = \{\sigma_i \ni 1 \leq i \leq v\}$ and abuse notation slightly by replacing each orbit in σ with a representative element $x_i \in \sigma_i \subset X$. We then have

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

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

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

since $Xg = \{x \in X \ni gx = x\} = \emptyset$ unless $g = e$, and $X_e = X$.

5.2 Sylow Theory

Recall Lagrange's theorem: If $H \leq G$ and G is finite, then $\#H \mid \#G$.

Consider the converse: if $n \mid \#G$, 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.

5.2.1 Class Functions

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

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

We can then separately count all orbits with exactly one element, which is exactly $X_G = \{x \in G \ni g \curvearrowright x = x \ \forall g$

We then have

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

for some j where $|Gx_i| > 1$ 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 $|Gx_i| = [G : G_{x_i}]$ for $j \leq i \leq v$, and $|Gx_i| > 1$ implies that $Gx_i \neq G$ and thus $p \mid [G : Gx_i]$. 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

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

But then, by the previous theorem, we have $|Z(G)| \equiv |X| \equiv |G| \mod p$, but since $Z(G) \leq G$ we have $|Z(G)| \cong 0 \mod p$, and 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.

5.2.2 Cauchy's Theorem

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

Proof: Consider $X = \{(g_1, g_2, \cdots, g_p) \in G^{\oplus p} \ni g_1 g_2 \cdots g_p = e\}$. 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 $|X| = |G|^{p-1}$.

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

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 $p \mid \left| X_{\langle \sigma \rangle} \right|$. So there is some $a \in G$ such that $a^p = 1$. Moreover, $\langle a \rangle \leq G$ is a subgroup of size p.

5.2.3 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? $G_x = G_H = \{g \in G \ni gHg^{-1} = H\}$, making G_H the largest subgroup such that $H \trianglelefteq G_H$. So we define $N_G(H) = G_H$.

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

By a previous theorem, $|G/H| = |S| = |S_H| \mod p$, where $|G/H| = [G : H]$. What is S_H? Thus is given by $S_H = \{x + H \in S \ni xHx^{-1} \in H \forall h \in H\}$. Therefore $x \in N_G(H)$.

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

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

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

6 Appendix

6.0.1 Big List of Notation

$$\begin{aligned}
C(x) &= & \left\{g \in G : gxg^{-1} = x\right\} && \subseteq G && \text{Centralizer} \\
C_G(x) &= & \left\{gxg^{-1} : g \in G\right\} && \subseteq G && \text{Conjugacy Class} \\
G_x &= & \{g.x : x \in X\} && \subseteq X && \text{Orbit} \\
x_0 &= & \{g \in G : g.x = x\} && \subseteq G && \text{Stabilizer} \\
Z(G) &= & \left\{x \in G : \forall g \in G,\ gxg^{-1} = x\right\} && \subseteq G && \text{Center} \\
\mathrm{Inn}(G) &= & \left\{\phi_g(x) = gxg^{-1}\right\} && \subseteq \mathrm{Aut}(G) && \text{Inner Aut.} \\
\mathrm{Out}(G) &= & \mathrm{Aut}(G)/\mathrm{Inn}(G) && \hookrightarrow \mathrm{Aut}(G) && \text{Outer Aut.} \\
N(H) &= & \left\{g \in G : gHg^{-1} = H\right\} && \subseteq G && \text{Normalizer}
\end{aligned}$$

7 Lecture 4: TODO

8 Lecture 5 (Tuesday 8/27)

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 $p \,\Big|\, [G : H]$ then $N_G(H) \neq H$.

8.1 Sylow Theorems

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

8.1.1 Sylow 1

Motto: 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: $|\phi^{-1}(K)| = p^{i+1}$.

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

Definition: For G a finite group and $|G| = p^n m$ where $p \not\Big| \, m$. Then a subgroup of order p^n is called a Sylow p-subgroup. (By Sylow 1, these exist.)

8.1.2 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. $\mathcal{L} = G/P_1$. Then let P_2 act on $\mathcal{L}$ by $p_2 \curvearrowright (g + P_1) := (p_2 g) + P_1$.

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

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

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

So there exists a coset xP_1 such that $xP_1 \in \mathcal{L}_{P_2}$, and so $yxP_1 = xP_1$ for all $y \in P_2$.

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

8.1.3 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

- $r_p \cong 1 \mod p$.
- $r_p \, \Big| \, |G|$.
- $r_p = [G : N_G(P)]$

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 the same old theorem, we have

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

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

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

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.

Then 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 $T = P$.

But 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 $G_p = N_G(P)$.

8.1.4 Applications

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:

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

> 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 $r_p \cong 1 \mod p$, $p \not\Big| \; r_p$, 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.

2. Let $|G| = 45$, then G is not simple. (Exercise)

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

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

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

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 $H \neq K, |H \bigcap K| < 16$. The order has to divides 16, so we in fact have $|H \bigcap K| \leq 8$. 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 $|H \bigcap K| = 8$. 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 $N_G(H \bigcap K) = G$, and so $H \bigcap K \trianglelefteq G$.

8.2 Classification of groups of a certain order

We have a classification of finite abelian groups (see table)

9 Lecture 6

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

9.1 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's a "recipe" for proving you have a direct product of groups:

Lemma: 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

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

and (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 $o(b) = p$ (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 $r_p \Bigm| |G| = pq$, 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 $r_q \Bigm| pq$, 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.

9.2 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.

9.3 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.

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. $A = \{x\} \implies F[A] = \{x^n \ni n \in \mathbb{Z}\} \cong \mathbb{Z}$.
2. $A = \{xy\} = \mathbb{Z} * \mathbb{Z}$ (not defined yet!). Note that there are not relations, i.e. $xyxyxy$ is reduced. To abelianize, we'd need to introduce a 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 $A = \{A_i\}\, i \in I$ 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 $\varphi(a_i) = a_i$. This is onto exactly because $G' = \langle a_i \rangle$, and using the theorem above we're done.

9.4 Generators and Relations

Let G be a group and $A \subseteq G$ be a generating subset so $G = \langle a \mid a \in A \rangle$. 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 $\ker\phi = \langle x^3 \rangle$.

Let $G = \mathbb{Z} \oplus \mathbb{Z}$, then $G \cong \langle x, y \mid [x, y] = 1 \rangle$.

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.

10 Lecture 7 (Thursday 29th)

Recall the table of distinct small groups we had:

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, $F[A]$. (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: $\mathbb{Z} * \mathbb{Z} = \langle x, y \mid xyx^{-1}y^{-1} = e \rangle$ where $x = (1, 0), y = (0, 1)$.

10.1 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 $b^2 \in \{e, a, a^2\}$. 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 $G = \langle a, b \mid a^3 = e, b^2 = e, bab^{-1} = a^2 \rangle$.

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:

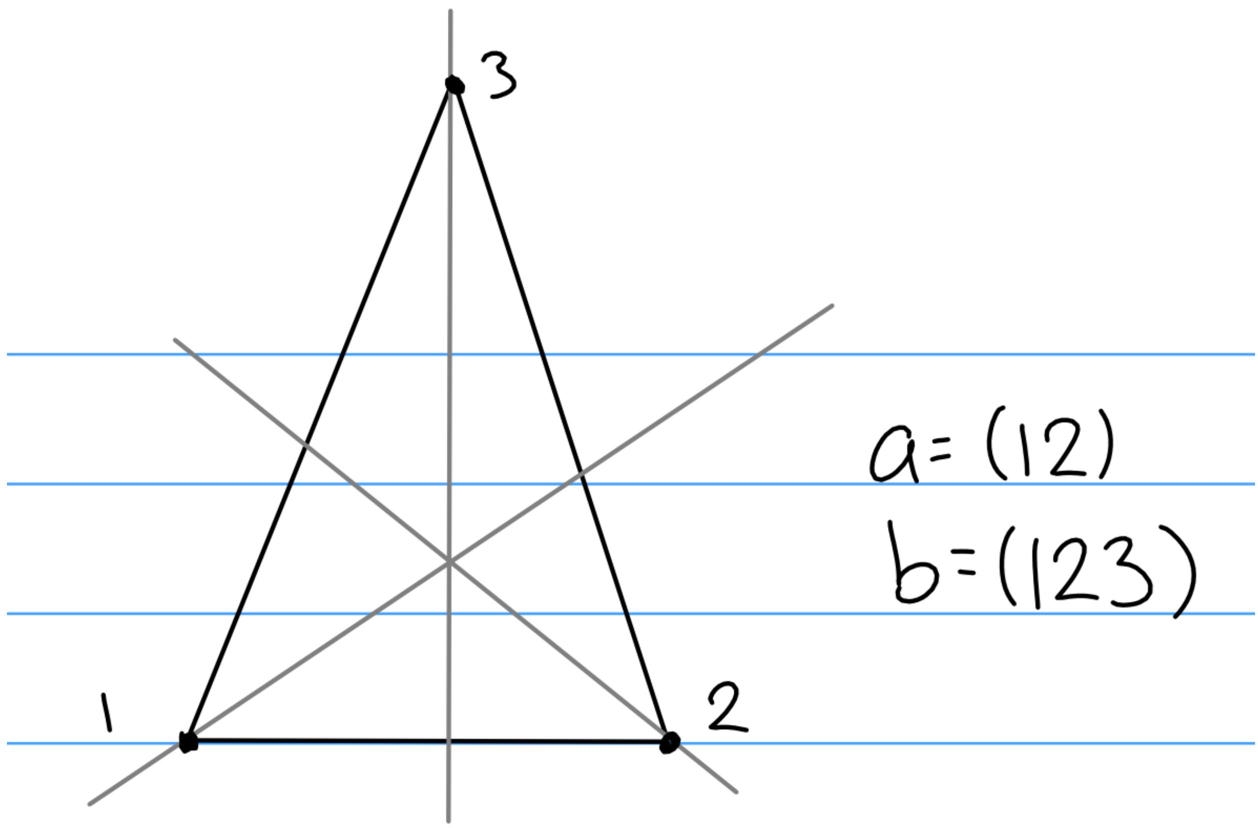


Figure 1: Image

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

For order 10, a similar argument yields

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

10.2 Groups of Order 8

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

Assume all elements have order 1,2. Let $a, b \in G$, consider $(ab)^2 = abab \implies ab = b^{-1}a^{-1} = ba$, so 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 options!)

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:

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

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).

10.3 Some Nice Facts

- If and $\phi : G\ toG'$, then
  - $N \trianglelefteq G \implies N \trianglelefteq \phi(G)$, although not necessarily 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.

10.4 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".

10.5 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:

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

11 Lecture 8: 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): 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 as a maximal normal subgroup.

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

Proof: Apply Schreier's refinement theorem.

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.

11.1 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 $[G, G] \trianglelefteq G$ and $G/[G, G]$ is abelian. Also, $[G, G]$ is the smallest normal subgroup such that the quotient is abelian, i.e. if $H \trianglelefteq G$ and G/N is abelian then $[G, G] \leq N$.

Proof:

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.

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,

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

3. The quotient is abelian

Let $H = [G, G]$. We have $aHbH = (ab)H$ and $bHaH = (ba)H$. But $abH = baH$ because $(ba)^{-1}(ab) = a^{-1}b^{-1}ab \in [G, G]$.

4. 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 $[G, G] \subseteq N$.

11.2 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.

12 Another Lecture: On to 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 $ab = ba = 1$.

A ring with unity is a *division ring* iff every nonzero element is a unit. A division ring is said to be a *field* iff it is commutative.

Suppose that $a, b \neq 0$ with $ab = 0$. Then a, b are said to be *zero divisors*. A commutative ring without zero divisors is an *integral domain*.

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 $ab = ac,\ a \neq 0 \implies b = c$.

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: (Similar to a 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 $a_j D = \{a_j x \ni x \in D \setminus \{0\}\}$.

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. $\square$.

12.1 Extension Fields

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

We can consider

$$\mathrm{Aut}(E/F) = \{\sigma : E \circlearrowleft \ni f \in F \implies \sigma(f) = f\},$$

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

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

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 $\psi : F \to E$ by $\psi(a) = a + (p)$. 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: $\mathbb{R}[x]/(x^2 + 1) \to \mathbb{R} \cong \mathbb{C}$ as fields.

12.2 Algebraic and Transcendental Elements

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.

Theorem: Let $F \leq E$ be a field extension and $\alpha \in E$. Define $\phi_\alpha : F[x] \to E$ by $\phi_\alpha(f) = f(\alpha)$; this is a homomorphism of rings and referred to as the *evaluation homomorphism*. 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.

12.3 Minimal Polynomial

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. $\square$

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.

13 Lecture ?

13.1 Vector Spaces

Definition: Let $\mathbb{F}$ be a field. A *vector space* is an abelian group 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: $\mathbb{R}^n, \mathbb{C}^n, F[x] = \text{span}(\{1, x, x^2, \cdots\}), L^2(\mathbb{R})$

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* if $\sum \alpha_i \mathbf{w}_i = \mathbf{0} \implies \alpha_i = 0$ 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.

> Note 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.

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.

13.2 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 $\{1, \beta, \beta^2, \cdots\}$ 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. Suppose $\beta \in F(\alpha)$. Then $\deg \min(\beta, F) \Bigm| \deg \min(\alpha, F)$.

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

Theorem: Let $E \geq F$ be algebraic, then $[E : F] < \infty \iff E = F(\alpha_1, \cdots, \alpha_n)$ for some $\alpha_n \in E$.

13.3 Algebraic Closures

Definition: Let $E \geq F$, and define $\overline{F_E} = \{\alpha \in E \ni \alpha \text{ is algebraic over } F\}$ to be *the algebraic closure of F in E*.

Example: $\mathbb{Q} \leq \mathbb{C}$, and $\overline{\mathbb{Q}} = \overline{\mathbb{R}_{\mathbb{C}}}$ the algebraic numbers (?).

Claim: $\overline{F_E}$ is a field.

Proof:G Let $\alpha, \beta \in \bar{(}F_E)$, so $[F(\alpha, \beta) : F] < \infty$. Then $F(\alpha, \beta) \subseteq \overline{F_E}$ is algebraic over F and $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta} \in F(\alpha, \beta)$. So $\bar{(}F_E)$ is a subfield of E.

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 $E = F$.

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 $\exists M \ni z \in \mathbb{C} \implies |f(z)| \leq M$. Entire means analytic everywhere.

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

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

13.4 Geometric Constructions:

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

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

14 Tuesday Lecture

Today: 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 is relatively easy. Showing closure under products:

Image

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

(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.

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

Corollary: Let $\gamma \in \mathcal{C}$ be constructible. Then there exist $\{\alpha_i\}_{i=1}^n$ such that $\gamma = \prod \alpha_i$, $[\mathbb{Q}(\alpha_1, \cdots, \alpha_j) : \mathbb{Q}(\alpha_1, \cdots, \alpha_{j-1})] = 2$, 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, $\cos 20°$ would be as well. There is an identity $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$. Letting $\theta = 20°$ so $3\theta = 60°$, we obtain

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

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

14.1 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, char $F = 0, p$ where p is 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 $F = p$, $\mathbb{Z}_p \subset F$.

Theorem: Let $E \geq F$ where $[E : F] = n$ and F is finite. If $|F| = q$, then $|E| = q^n$.

Proof: E is a vector space over F. Let $\{v_i\}^n$ be a basis. Then $\alpha \in E \implies \alpha = \sum^n a_i v_i$ 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 $\alpha\alpha^{p^n-1} = \alpha 1 \implies \alpha^{p^n} = \alpha$. $\square$.

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 $E = F(\alpha)$. $\square$

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 $E \geq F$. So 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 α 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.

15 Lecture (Tuesday)

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.

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

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 $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} - \alpha\beta$ and $\alpha^{-p^n} = \alpha^{-1}$. So K is a field and $|K| = p^n$.

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 $K := \{\alpha \in F \ni \alpha^{p^n} - \alpha = 0\}$.

We also have $F = \left\{\alpha \in \overline{F} \ni \alpha^{p^n} - \alpha = 0\right\}$. Moreover, $p^{rs} = p^r p^{r(s-1)}$. Let $\alpha \in F$. Then $\alpha^{p^r} - \alpha = 0$.

So 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 equal 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 $f(x)$. $\square$

15.1 Simple Extensions

Let $\phi_\alpha : F[x] \to E$ where $F \leq E$ be the evaluation map, i.e $\phi_\alpha(f(x)) = f(\alpha)$.

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 for $F[x]/\min(\alpha, F)$. 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 $\beta = \sum_{i=0}^{n-1} c_i \alpha^i$ where $n = \deg \min(\alpha, F)$.

Proof:

Existence:

We have $F(\alpha) = \left\{ \sum_{i=1}^{r} \beta_i \alpha^i \ni \beta_i \in F \right\}$. 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:

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

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. $\square$

Note that 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 that adjoining any root of a minimal polynomial will yield isomorphic (usually not identical) fields. These are distinguished as subfields of (say) 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, then $\left\{1, \alpha, \cdots, \alpha^{n-1}\right\}$ is a basis for $F(\alpha)$ over F. Moreover, if $\beta \in F(\alpha)$, then β is also algebraic over F and $\deg \min(\beta, F) \;\Big|\; \deg \min(\alpha, F)$.

Proof:

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. $\square$

15.2 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 $\zeta = \exp(2\pi i/3)$.
- $\alpha = a + bi \in \mathbb{C}$ has conjugate $a - bi$, and $\min(\alpha, \mathbb{R}) = x^2 - 2ax + (a^2 + b^2)$

16 Lecture Thursday

16.1 Conjugates

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

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

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

Proof: Suppose ϕ is an isomorphism. Let $f \coloneqq \min(\alpha, F) = \sum c_i x^i$ 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 $f = \min(\alpha, F) \,\Big|\, \min(\beta, F)$.

But we can repeat this argument with f^{-1} and $g(x) \coloneqq \min(\beta, F)$, 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 $\phi(x + y) = \phi(x) + \phi(y)$ 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 $z = 0$. $\square$

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 if $f(a + bi) = 0$. This isomorphism commutes with f, so we have $0 = \psi(f(a + bi)) = f(\psi(a - bi)) = f(a - bi)$.

16.2 Fixed Fields and Automorphisms

Definition: Let F be a field and $\psi : F\circlearrowleft$ is an *automorphism* iff ψ is an isomorphism (note that the domain and range are the same).

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

$$E_I = \{\alpha \in E \ni \sigma(a) = a \ \forall \sigma \in I\}$$

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

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 $A = \{\sigma : E\circlearrowleft \ni \sigma \text{ is an automorphism }\}$. Then A is a group under function composition.

Theorem: Let E/F be a field extension, and define $G(E/F) = \{\sigma : E\circlearrowleft \ni f \in F \implies \sigma(f) = f\}$. Then $G(E/F) \leq A$ is a subgroup which contains F.

Proof: This contains the identity function, 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 $f \in F$.

17 Tuesday, October 1

Today: 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 $f \in F$.

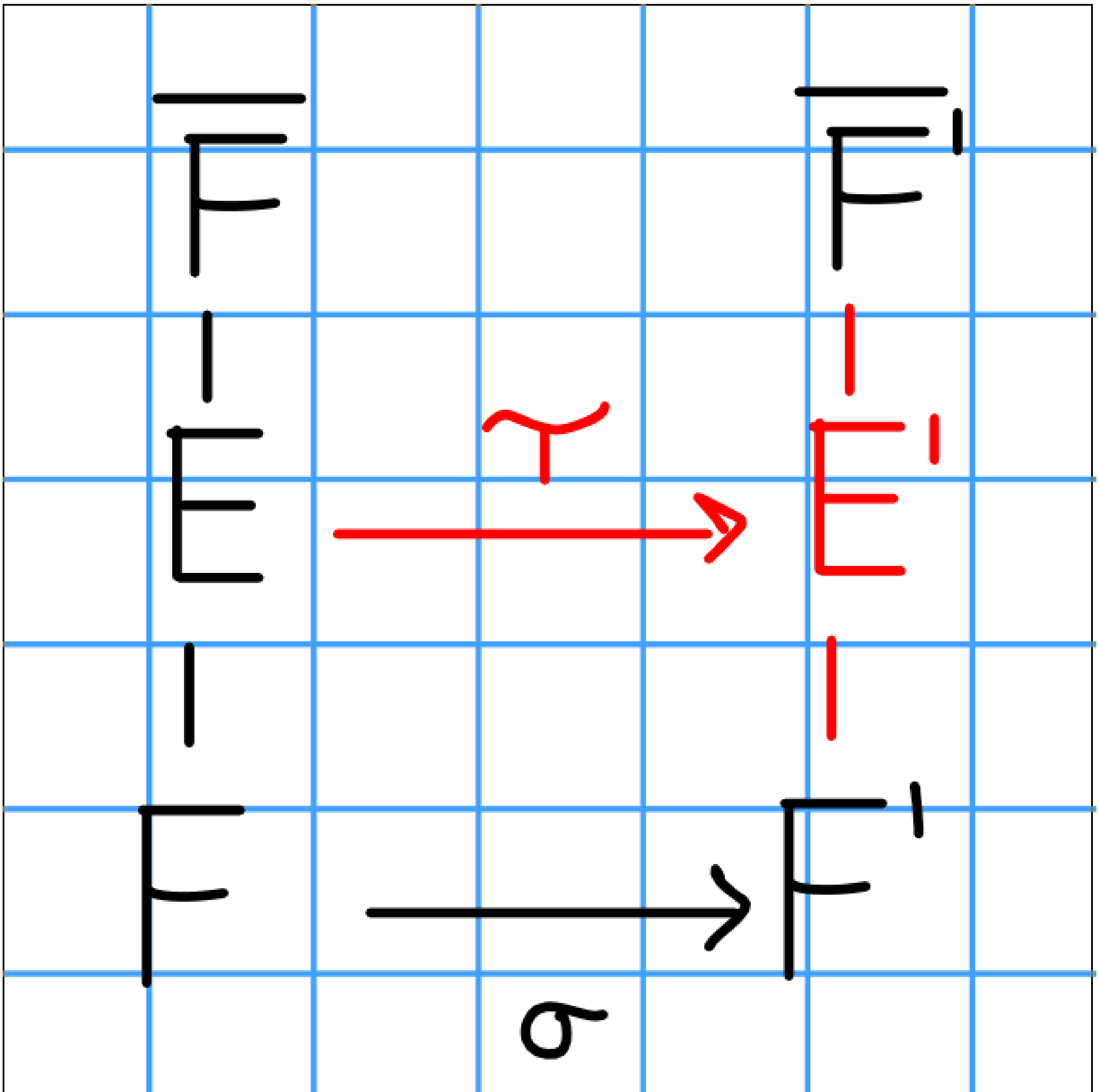
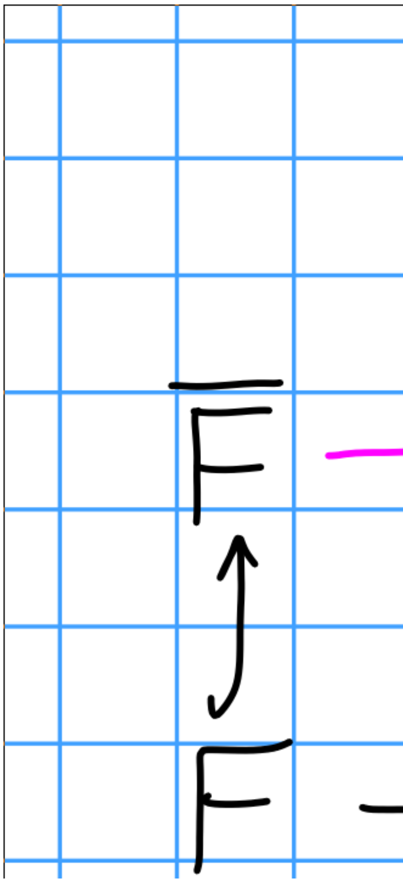


Figure 2: Image

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 $\overline{F}' = \tau(\overline{F})$.
$\square$

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:

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

> 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 $G(E/F) := \mathrm{Gal}(E/F)$; 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*.

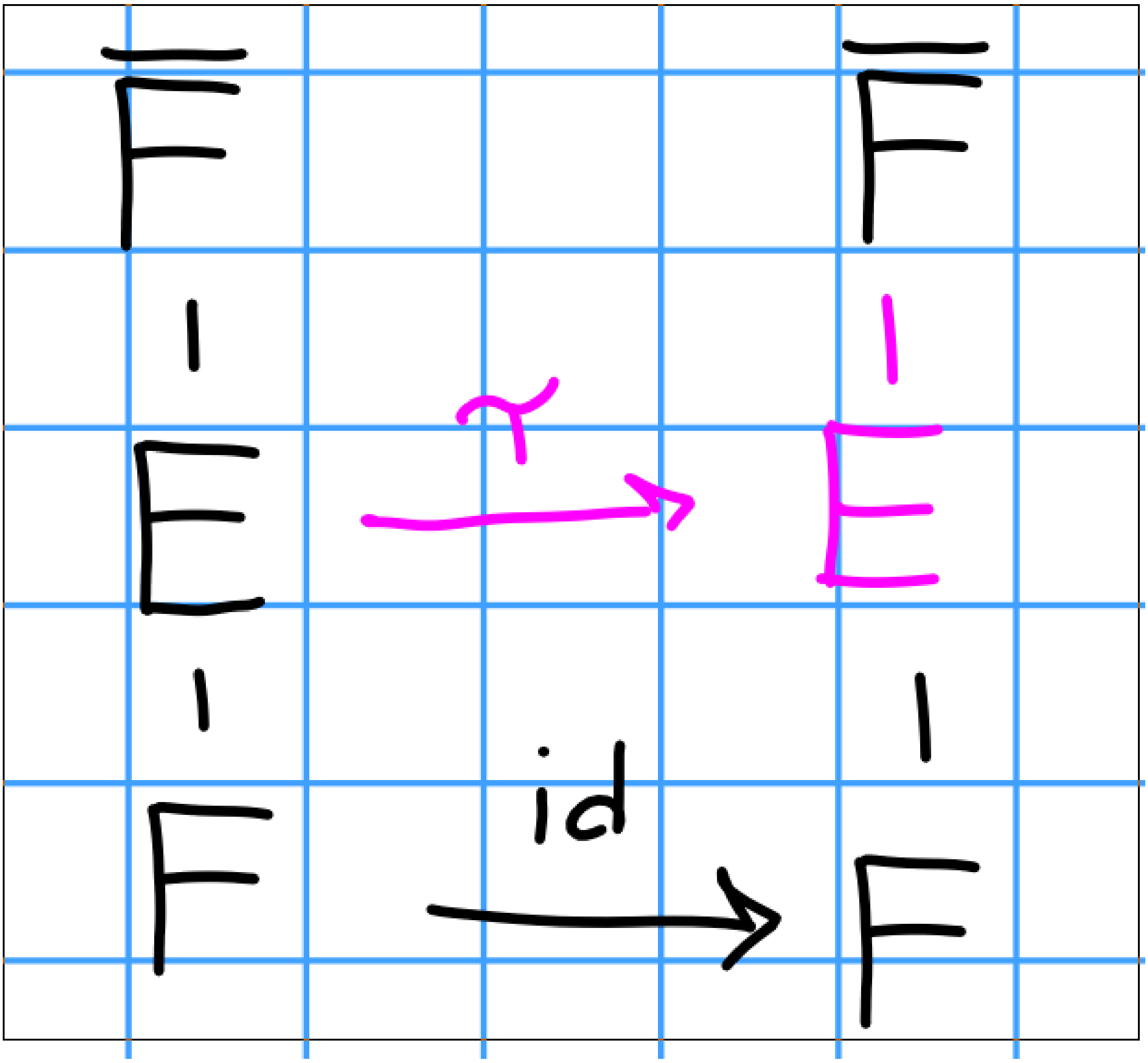


Figure 3: Image

Proof: Since $[E:F]$ is finite, we have $F_0 := F(\alpha_1, \alpha_2, \cdots, \alpha_t)$ 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

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

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 $\sigma_1 : (\sqrt{2}, \sqrt{5}) \mapsto (-\sqrt{2}, \sqrt{5})$ and $\sigma_2 : (\sqrt{2}, \sqrt{5}) \mapsto (\sqrt{2}, -\sqrt{5})$, as well as $\mathrm{id}, \sigma_1 \circ \sigma_2$. Thus $\mathrm{Gal}(E/F) = \mathbb{Z}_2^2$.

17.1 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 $(x - \alpha)^\nu \mathrel{\Big|} f$ 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:

This induces a map $F(\alpha)[x] \xrightarrow{\tau} F(\beta)[x]$ which sends $\sum c_i x^i \mapsto \sum \psi(c_i) x^i$, 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 $\mathrm{mult}(\alpha) \leq \mathrm{mult}(\beta)$. But repeating the argument with α, β switched yields the reverse inequality, so they are equal. $\square$

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

Figure 4: Image

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 $\{E : F\} \mid [E : F]$.

18 Thursday October 3

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

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

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 and $\{F(\alpha) : F\} \mid [F(\alpha) : F]$.

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

Proof: If $E \geq F$ is finite, $E = F(\alpha_1, \cdots, \alpha_n) := F$. Then $\min(\alpha_i, F)$ has a_j as a root, n_j distinct roots, and v_j common multiplicities? Then $[F : F(\alpha_1, \cdots, \alpha_{n-1})] = n_j v_j = v_j\,\{F : F(\alpha_1, \cdots, \alpha_{n-1})\}$. Then $[E : F] = \prod n_j v_j$ and $\{E : F\} = \prod n_j$, so we obtain divisibility.

Definitions:

1. $E \geq F$ is *separable* iff $[E : F] = \{E : F\}$
2. $\alpha \in E$ is *separable* iff $F(\alpha) \geq F$ is separable.
3. $f(x) \in F[x]$ 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 $f(x) = c \min(\alpha, F)$ for some constant $c \in F$, 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 is separable over F iff every $\alpha \in E$ is separable over F.

Proof: 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.

Conversely, 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. It is separable over F iff $\min(\alpha_2, F)$ has roots of multiplicity one. Then $\min(\alpha_2, F(\alpha_1)) \mathrel{\Big|} \min(\alpha_2, F)$. So $\min(\alpha_2, F(\alpha))$ has roots of multiplicity one. So $F(\alpha_1, \alpha_2)$ is separable over $F(\alpha_1)$.

18.1 Perfect Fields

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

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 $(x - \alpha) \mathrel{\Big|} f'$.

Conversely, 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. Then

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

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

Thus we can 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 $\mathrm{char}(F) = 0$, 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 $\min(\alpha, F) \mid f(x)$. 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. $\square$

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

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.

19 Tuesday October 8

19.1 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 $\{f_i(x) \in F[x] \ni i \in I\}$ 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 $\{x^{-}2, x^2 - 5\}$.
- $\mathbb{C}$ is a splitting field for $\{x^2 + 1\}$.
- $\mathbb{Q}(\sqrt[3]{2})$ 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 $\{f_i(x) \ni f_i(x) \in F[x], i \in I\}$. Then $E = \langle \alpha_j \mid j \in J \rangle$ 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 $p(x) = 0, 0 \in F \implies 0 = \sigma(p(\alpha_j)) = \sum a_i \sigma(\alpha_j)^i$. Thus $\sigma(\alpha_j)$ is a conjugate, and thus a root of some $f_i(x)$.

$\Longleftarrow$: Suppose any isomorphism of E leaving F fixed is an automorphism. Let $g(x)$ be an irreducible polynomial and $\alpha \in E$ a root.

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 $S = \{g_i(x) \in F[x] \ni g_i \text{ irreducible and has a root in } E\}$. This defines a splitting field for $\{g_j\}$, and we're done. $\square$

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. $|\mathrm{Gal}(E/F)|$.

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

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 $x^{p^n} - x$.

Examples:

1. $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ is a degree 4 extension, the number of automorphisms was 4, and the Galois group was $\mathbb{Z}_2^2$.

2. E the splitting field of $x^3 - 3$ over $\mathbb{Q}$, which 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 $\min(\sqrt[3]{3}, \mathbb{Q}) = x^3 - 3, \min(\zeta_3, \mathbb{Q}) = x^2 + x + 1$, and thus this is a degree 6 extension. Since $\mathrm{char}\mathbb{Q} = 0$, we have $[E : \mathbb{Q}] = \{E : \mathbb{Q}\}$ for free. We know that any automorphism has to map $\sqrt[3]{3} \mapsto \sqrt[3]{3}$, $\sqrt[3]{3}\zeta_3$, $\sqrt[3]{3}\zeta_3^2$ and $\zeta_3 \mapsto \zeta_3, \zeta_3^2$. You can show this is nonabelian by composing a few of these; thus the Galois group is S^3.

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.

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

Figure 5: Image

19.2 Galois Correspondence

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

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 $\sigma, \tau \in \mathrm{Gal}(K/F)$, $\sigma \mid_E = \tau \mid_E$ iff σ, τ are in the same left coset of $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$.

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.

Proof of (2):

Image

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 $\tau^{-1}\sigma := \mu$. Note that μ fixes E by definition. Then $\sigma = \tau\mu$, and so $\sigma(e) = \tau(\mu(e)) = \tau(e)$ for all $e \in E$.

> 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 $K = \mathbb{Q}(\sqrt[3]{3}, \zeta_3), E = \mathbb{Q}(\sqrt[3]{3}), F = \mathbb{Q}$. Then $K \trianglelefteq E, K \trianglelefteq F$, but $E \not\trianglelefteq F$.