Modern Algebra

MATH 504, University of Washington, Autumn 2021

These lecture notes are for MATH 504, "Modern Algebra," taught by Julia Pevtsova at The University of Washington during Autumn 2021. These notes are written by Tony Zeng using Jackson Petty's `coursework-latex` repository. These notes are not official and have not been proofread by the instructor for the course. Please report any mistakes to me at `txz@uw.edu`.

Contents

1 September 29, 2021

Group

Definition (Group)**.** A group G is a set with a binary operation $\mu : G \times G \to G$ denoted by

$$\mu(a, b) \mapsto ab.$$

Many symbols are used: $\times, \cdot, +, *$. A group with its operation satisfies the following axioms.

1. Associativity.
2. There is a 2-sided unit e

$$ea = ae \quad \forall a \in G.$$

3. There is a 2-sided inverse.

$$\forall a \in G \quad \exists a^{-1} : a^{-1}a = aa^{-1} = e$$

Remark 1.1 — OK to ask for only 1-sided unit/inverse.

Remark 1.2 — A monoid satisfies 1. and 2. but has no inverse.

Example 1.1. Examples of groups.

1. $\mathbb{R}^+, \mathbb{Z}^+, \mathbb{Q}^+, \mathbb{C}^+, Q^+$.
2. Trivial group. $G = \{e\}$.
3. $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$. $(\mathbb{R}^\times, \cdot)$.
4. $\mathbb{Z}/n\mathbb{Z}$, modular arithmetic.
5. $\mathbb{Z}/p\mathbb{Z}$, with p prime, under multiplication.
6. General linear group. $GL_n(\mathbb{R})$, invertible $n \times n$ matrices with real entries. Alternatively,

$$\{A \in A_n(\mathbb{R}) \mid \det A \neq 0\}$$

   We can replace $\mathbb{R}$ with any field $(GL_n(\mathbb{Q}), GL_n(\mathbb{C}))$.
7. $GL_n(\mathbb{Z})$, invertible $n \times n$ matrices with integer entries. Note that this is OK since we take "inverse" to enforce integer entries.
8. Special linear group. $SL_n(\mathbb{R})$. Alternatively,

$$\{A \in A_n(\mathbb{R}) \mid \det A = 1\}.$$

   This is a group, since $\det$ respects multiplication. Again, we can replace $\mathbb{R}$ with any field.

9. Orthogonal group. $O_n(\mathbb{R})$ is

$$\{A \in GL_n(\mathbb{R}) \mid AA^T = I_n\}.$$

10. S_n.
11. D_n.

2 October 1, 2021

Example 2.1. Permutation group. For a set X, we define $S(X)$ to be the permutation group of X.

$$S(X) = \{\varphi : X \to X\}$$

where φ is a bijection. The operation of this group is function composition.

$$X \to^{\varphi} X \to^{\psi} X$$

$$X \to^{\psi \circ \varphi} X$$

The identity is simply the identity function. We commonly use $X = \{1, \dots, n\}$, in which case $S(X) = S_n$, the symmetric group.

Definition (Abelian group)**.** We say a group G is **abelian** if the group operation is commutative, *Abelian group*

$$ab = ba \quad \forall a, b \in G.$$

Terminology:

$$a, b \in G \mapsto [a, b] = a^{-1}b^{-1}ab$$

The commutator vanishes iff a, b commute. Therefore, G is abelian iff all commutators vanish.

Terminology:

The order of G, denoted $|G|$, is the number of elements in G (could be ∞). An element $a \in G$ has order n, where n is the minimal positive integer such that $a^n = e$.

2.1 Groups of Small Order

Let's look at groups of small order.

Order	Groups
1	e
2	$\{1, -1\} \subset \mathbb{R}^\times, \mathbb{Z}^\times, S_2, \mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$S_3, \mathbb{Z}/6$
7	$\mathbb{Z}/7\mathbb{Z}$
8	$Q_8, D_4, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}$

Question 2.1 — How many monoids of order 8?

Answer is 858,977.

2.2 Subgroups

Subgroup

Definition (Subgroup)**.** A subset $H < G$ is a **subgroup** if it is closed under multiplication (same operation as G), unit, and inverse. That is, if $a, b \in H$,

- $ab \in H$
- $e \in H$
- $a \in H \Rightarrow a^{-1} \in H$

Example 2.2. If $a \in G$, consider the subgroup

$$\langle a^n \mid n \in \mathbb{Z} \rangle < G.$$

This is called the "cyclic"subgroup. We say that this subgroup is "generated" by a.

Terminology:

We will use $<$ to denote subgroup relation and $\subset$ to denote subset relation. If $X, Y \subset G$, we say

$$X \cdot Y = \{xy \mid x \in X, y \in Y\}$$

Properties:

1. $H < G$ implies $H \cdot H \subset H$ and $H^{-1} \subset H$.
2. Note
$$H < G \Leftrightarrow \begin{cases} H \neq \varnothing \\ H \cdot H^{-1} \subset H \end{cases}$$
3. Intersection of subgroups is a subgroup.

Proof. 1. and 3. as exercises.

Proving 2. $\Leftarrow$.

1. $H \neq \varnothing$ means we have some $a \in H$. Then $a \cdot a^{-1} = e \in H$, so $H \cdot H^{-1} \subset H$.
2. $a, b \in H$ means $b^{-1} = eb^{-1} \in H$ and $ab = a(b^{-1})^{-1} \in H$.

■

2.3 Generators

Minimal subgroup

Definition (Minimal subgroup)**.** If $S \subset G$, we say that $\langle S \rangle$ is the **minimal subgroup** of G containing S (minimal with respect to inclusion). $\langle S \rangle$ is generated by S. In practice,

$$S = \{s_1, s_2, \ldots\}$$
$$\langle S \rangle = \left\{ \prod_{\text{finite}} s_i \text{ and inverses } \mid s_i \in S \right\}$$

Example 2.3. If $a \in G$, consider

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\},$$

the cyclic group generated by a.

Definition. Generation terminology.

1. For $S \subset G$, we say S generates G if $\langle S \rangle = G$.
2. A group is cyclic if it is generated by a single element, that is $G = \langle a \rangle$ for some $a \in G$.
3. $S \subset G$ is a minimal set of generators for G if $\langle S \rangle = G$ and no proper subset of S generates G.

2.4 Homomorphisms

Definition. $f : G \to H$ is a **group homomorphism** if

$$f(ab) = f(a)f(b)$$

for all $a, b \in G$.

Remark 2.1 — Homomorphisms preserve identity and inverses.

Definition. Given homomorphism $f : G \to H$,

1. f is a **monomorphism** if it is injective,
2. f is an **epimorphism** if it is surjective,
3. and f is an **isomorphism** if there exists $f^{-1} : H \to G$ such that $f \circ f^{-1} = \mathrm{id}_H$ and $f^{-1} \circ f = \mathrm{id}_G$. Equivalently, it is both a monomorphism and an epimorphism.

Composition of homorphisms

$$G \to^f H \to^h L$$

$$G \to^{H \circ f} L$$

3 October 4, 2021

Remark 3.1 — We will use the inverse existence definition of isomorphisms more, since the other relies on more set theoretic structure.

Kernel

Definition (Kernel)**.** The **kernel** of a homomorphism $f : G \to H$ is the preimage of the identity.

$$\mathrm{Ker} f = \{g \in G \mid f(g) = e\} < G$$

The **image** of f is

$$\mathrm{Im} f = \{h \in H \mid \exists g \in G : f(g) = h\} < H.$$

(Verify subgroup claims.)

Lemma 3.1. *For homomorphism $f : G \to H$,*

1. *f is a monomorphism $\Leftrightarrow$ $\mathrm{Ker} f = e$.*
2. *f is an epimorphism $\Leftrightarrow$ $\mathrm{Im} f = H$.*

Example 3.1.

1. Denote $\mathrm{tr} = \{e\}$. $\mathrm{tr} \to G$ and $G \to \mathrm{tr}$.
2. Id: $G \to G$ with $g \mapsto g$.
3. For $a \in G$, $\mathbb{Z} \to G$ by $n \mapsto a^n$. If $\mathrm{Im} f = \langle a \rangle \subset G$ cyclic subgroup of G. When is f a monomorphism? When a has infinite order.
4. $G \to G$ with $a \mapsto a^n$, with $n \in \mathbb{Z}$ greater than 1. Is this a group homomorphism? When G is abelian.
5. $GL_n(\mathbb{R}) \to \mathbb{R}^\times$ via the determinant, $A \mapsto \det A$.

$$\mathrm{Ker} GL_n(\mathbb{R}) = SL_n(\mathbb{R})$$

Lemma 3.2. *Let G by a cyclic group. Then any subgroup and any homomorphic image of G is cyclic.*

Theorem 3.3 (Cayley)**.** *Let G be a finite group. Then there exists a monomorphism $f : G \hookrightarrow S_n$ for some n.*

Proof. Let $n = |G|$, and $S_n = S(G)$. Consider $f : G \to S(G) = \{\varphi : G \to G\}$ with

$$g \mapsto \sigma_g : G \to G$$

where σ_g sends $a \mapsto ga$. Take $\{g_1, \ldots, g_n\}$ all elements of G. Then

$$\sigma_g(g_1, \ldots, g_n) \mapsto (gg_1, \ldots, gg_n)$$

Need to show that

1. σ_g is a bijection, and
2. f is a homomorphism, and
3. f is a monomorphism.

■

3.1 *Cosets, normal subgroups, factor groups*

Coset

Definition (Coset)**.** For $H < G$ and $y \in G$,

$$yH = \{yh \mid h \in H\}$$

is the left **coset** of H with respect to y. Right coset defined analogously.

Lemma 3.4. *TFAE. For $H < G$ and $x, y \in G$,*

1. $xH = yH$,
2. $y \in xH$,
3. $x^{-1}y \in H$, *and*
4. $xH \cap yH \neq \varnothing$.

Corollary 3.5. *$xH = yH$ defines and equivalence relation on G.*

Let G/H denote the set of equivalence classes (set of left cosets yH).

> Remark 3.2 — $H\backslash G$ for set of right cosets).

Index

Definition (Index)**.** The **index** of H in G is $[G : H] = |G/H|$.

> Remark 3.3 — There exists a bijection
>
> $$H\backslash G \to^{Hy \mapsto y^{-1}H} G/H.$$
>
> In particular,
>
> $$[G : H] = |H\backslash G|.$$

Proposition 3.6. *For $H < G$ finite,*

$$|G| = |G : H| \cdot |H|$$

Proof. Counting.

$$G = \coprod yH$$

over representatives y of G/H (or over set of coset representatives). $|yH| = |H|$, so

$$|G| = |G/H| \cdot |H| = |G : H| \cdot |H|$$

■

Theorem 3.7 (Lagrange)**.** *Let $H < G$ finite. Then*

$$|H| \mid |G|$$

In other words, H divides G.

Corollary 3.8. *If $a \in G$ with $|G| < \infty$, then $|a|$ divides $|G|$.*

Proof. Let $H = \langle a \rangle \subset G$.

$$|H| = |\langle a \rangle| = |a|$$

Apply Lagrange's theorem to H. ■

Definition (Normal)**.** $H < G$ is called **normal** if for all $g \in G$, *Normal*

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\} = H.$$

If H is normal, we write $H \triangleleft G$.

Remark 3.4 — $H \triangleleft G$ implies (equivalent actually)

1. $yH = Hy$ for all $Y \in G$, and
2. $g^{-1}Hg = H$.

4 October 6, 2021

Lemma 4.1. *For group homomorphism $f : G \to H$, the kernel of f is a normal subgroup.*

Example 4.1. $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$.

Theorem 4.2. *For $H \triangleleft G$, G/H has a group structure "induced" from G.*

Proof. Suppose we have cosets xH, yH. Then multiplication can be defined as $xHyH = xyH$. Why is this well-defined? Pick $x' = xh$ a different coset representative for xH. Then

$$(xh)H \cdot yH = xhyH = xyy^{-1}hyH = (xy)(y^{-1}hy)H = xyH$$

since $y^{-1}hy \in H$. Check for yH as well. Identity in G/H is just $eH = H$. Inverses are obtained simply by $(xH)^{-1} = x^{-1}H$. ■

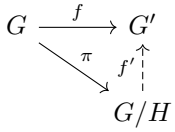
Definition (Factor group)**.** G/H is a **factor group** with respect to H. *Factor group*

Remark 4.1 — $H\backslash G$ is isomorphic to G/H where we send $Hx \mapsto x^{-1}H$.

For $H \triangleleft G$, consider the map $\pi : G \to G/H$ given by $g \mapsto gH$. We will also use the notation $gH = \overline{g}$.

The following is $\star$ abstract nonsense.

Proposition 4.3 (Universal property)**.** *For $H \triangleleft G$, suppose we have homomorphism $f : G \to G'$ sends H to the identity. Then there exists a unique $f'; G/H \to G'$ such that the following diagram commutes.*



That is, $f = f' \circ \pi$.

Proof. Exercise. ■

This ends the $\star$ abstract nonsense.

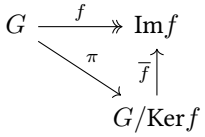
4.1 Isomorphism Theorems

Theorem 4.4. *For $f : G \to G'$ a homomorphism, then there exists $\overline{f}$*

$$G/Kerf \simeq Imf$$

Proof. Construct $\overline{f}$. We can write $f : G \to \mathrm{Im}f$ (or assume f is surjective). Note that $f(\mathrm{Ker}f) = e$. Then by the universal property, we have $\overline{f} : G/\mathrm{Ker}f \to \mathrm{Im}f$. $\overline{f}$ sends $\overline{g} \mapsto f(g)$.

1. $\overline{f}[$ is an epimorphism.



   $f = \overline{f} \circ \pi$. f is an epimorphism implies $\overline{f}$ is also an epimorphism.

2. f is a monomorphism. Suppose $\overline{f}(\overline{g}) = e$. Then $\overline{g} \in G/\mathrm{Ker}f$. Then we have $\overline{f}(\overline{g} = f(g) = e$.

$$\Rightarrow g \in \mathrm{Ker}f \Rightarrow \overline{g} = g\mathrm{Ker}f = \mathrm{Ker}f = \overline{e}$$

   in $G/\mathrm{Ker}f$.

■

Corollary 4.5. *$f : G \to G'$ implies*

$$G \twoheadrightarrow G/Kerf \simeq Imf \hookrightarrow G'$$

The following is ⋆ abstract nonsense.

Definition. An exact sequence of groups is a sequence

$$\to G_{i-1} \to^{f_{i-1}} G_i \to^{f_i} G_{i+1} \to^{f_{i+1}}$$

such that $\mathrm{Ker}f_i = \mathrm{Im}f_{i+1}$.

Short exact sequences. Here we use 1 to denote tr.

$$1 \to G_1 \to^f G_2 \to^g G_3 \to 1$$

Explicitly,

1. $\mathrm{Im}e = e = \mathrm{Ker}f$. f is a monomorphism.
2. $\mathrm{Im}f = \mathrm{Ker}g$.
3. g is an epimorphism.

Remark 4.2 — Abelian categories exist.

This ends the ⋆ abstract nonsense.

Example 4.2. Consider

$$0 \to \mathbb{Z} \to^{n} \mathbb{Z} \to \mathbb{Z}/n \to 0.$$

Notice that $\text{Ker} g = n\mathbb{Z} = \text{Im}\{n : \mathbb{Z} \to \mathbb{Z}\}$.

Example 4.3. Consider

$$1 \to SL_n(\mathbb{R}) \to GL_n(\mathbb{R}) \to^{\det} \mathbb{R}^{\times} \to 1$$

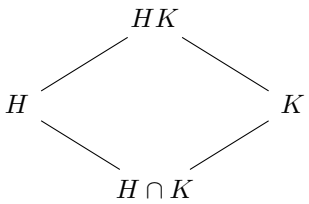
Example 4.4. Consider

$$0 \to \mathbb{R} \to^{\exp} \mathbb{R}^{\times} \to^{\text{sign}} \{1, -1\} \to 1.$$

Remark 4.3 — If $H \triangleleft G$, we can always write

$$1 \to H \to G \to G/H \to 1.$$

Theorem 4.6. *$H \triangleleft G$ and $K < G$. In the Hasse diagram,*



$HK/H \simeq K/H \cap K$.

Proof. Steps.

1. HK is a group
2. $H \triangleleft HK$
3. $H \cap K \triangle leftK$
4. $K \to HK/H, x \to xH$

■

5 October 8, 2021

Theorem 5.1 (Third Isomorphism Theorem)**.** *$H \triangleleft G$ with $T : G \to G/H$. There is a bijection between subgroups of G containing H and subgroups of G/H.*

$$H \triangleleft K < G \to K/H$$

If $K < G$ contains H, normal in G implies normal in K. For $H \triangleleft K \triangleleft G$,

$$K/H \triangleleft G/H$$

and $(G/H)/(K/H) \simeq G/K$.

Remark 5.1 — $H \triangleleft K \triangleleft G$ does not imply $H \triangleleft G$.

5.1 Group actions

Groups arose from studying symmetries.

Definition. G acts on a set X if we have a map $G \times X \to X$ with $(g, x) \mapsto gx$ that respects group structure.

$$\begin{array}{ccc} G \times G \times X & \xrightarrow{(g_1\ g_2\ x) \to (g_1 g_2\ x)} & G \times X \\ \downarrow{\scriptstyle (g_1\ g_2\ x) \to (g_1 g_2\ x)} & & \downarrow{\scriptstyle (g\ x) \to gx} \\ G \times X & \xrightarrow{(g\ x) \mapsto gx} & X \end{array}$$

Remark 5.2 — We can also have a right action. $X \times G \to X$.

Proposition 5.2. *There is a bijection between actions of G on X and group homomorphisms from G to $S(X)$.*

Proof. $g \in G$ gives an action $\sigma_g : X \to X$ with $x \mapsto gx$. $\sigma_g(x) = gx$ is a bijection since it has an inverse given by $\sigma_{g^{-1}}(x) = g^{-1}x$. Then $g \mapsto \sigma_g$ is a group homomorphism. Check rest. ∎

Definition (Orbit)**.** If G acts on X, then the **orbit** of G on $x \in X$ is *Orbit*

$$Gx = \{gx \mid g \in G\}$$

Remark 5.3 —

$$X = \coprod Gx$$

where we take disjoint union over x as orbit representatives. Orbits partition X.

Example 5.1.

1. G can act on itself, so take $X = G$. The action is simply left multiplication.
$$G \times G \to G \quad g \cdot x \mapsto gx$$
2. We can also define an action by
$$g \cdot h \mapsto hg^{-1}.$$
This actually redefines the left action.

Transitivity and faithfulness

Definition (Transitivity and faithfulness)**.** G acts on X **transitively** if for all $x, y \in X$, there exists a g such that $y = gx$, or equivalently, $X = Gx$ (only one orbit). G acts **faithfully** if the corresponding group homomorphism $G \hookrightarrow S(X)$ is injective.

Example 5.2.

3. Conjugation. $G \times G \to G$ with $G, h) \mapsto ghg^{-1}$.
4. $H < G$, take $X = G/H$. $G \times G/H \to G/H$ where $(g, \overline{x}) \mapsto \overline{gx}$.
$$g(xH) = (gx)H$$
is well defined.
5. Representation theory. Actions of groups on vector spaces. $G \times V \to V$.
$$g(\alpha v + \beta w) = \alpha gv + \beta gw$$
for α, β in your field and v, w in your vector space. Explicitly, matrix multiplication is an example.
$$GL_n(\mathbb{R}) \times \mathbb{R}^n \to \mathbb{R}^n$$

Isotropy group

Definition (Isotropy group)**.** $G \times X \to X, x \in X$. The **isotropy group** of x (or stabilizer) is
$$G_x = \{g \in G \mid gx = x\}$$

Remark 5.4 —

1. $G_x < G$ is a subgroup.
2. $G_{gx} = gG_xg^{-1}$.

Proposition 5.3. *For $G \times X \to X$, there is a bijection between $G/G_x \leftrightarrow Gx$.*

$$\overline{g} = gG_x \mapsto gx$$

Proof. Surjective by definition. Injective? Let $g, h \in G$. Suppose $gx = hx$. Then

$$h^{-1}gx = x \Rightarrow h^{-1}G \in G_x \Rightarrow hG_x = gG_x,$$

so we have injection. ■

Theorem 5.4 (Class formula)**.** *X finite.*

$$|X| = \sum |G : G_x|$$

where we are summing over x orbit representatives.

6 October 11, 2021

Proof. Note that

$$X = \coprod Gx,$$

the disjoint union of orbits. Therefore,

$$|X| = \sum |G_x|.$$

Last time, we had

$$|Gx| = |G : G_x|,$$

so

$$|X| = \sum |G : G_x|.$$

■

Example 6.1. For finite G, $X = 2^G$. G can act on X via conjugation.

$$G \times X \to X$$

$$g \cdot Y \mapsto gYg^{-1}$$

The following definition and remark reference the previous example.

Definition (Normalizer)**.** We call *Normalizer*

$$\text{stab}_G(H) = \text{Norm}_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

the **normalizer** of H, for $H < G$.

Remark 6.1 —

1. $H < G \Rightarrow \text{Norm}_G(H) < G$
2. $H \triangleleft \text{Norm}_G(H)$
3. $\text{Norm}_G(H) = G \Leftrightarrow H \triangleleft G$
4. $\text{Norm}_G(H)$ is the largest subgroup in G in which H is normal.

Definition (Centralizer)**.** The **centralizer** of an element x is *Centralizer*

$$C_g(x) = \text{Cent}_G(x) = \{g \in G \mid gxg^{-1} = x\}.$$

Example 6.2. Action of $G \times G \to G$ by conjugation, where orbits are conjugacy classes. Stabilizers are centralizers.

Definition (Center)**.** The **center** Z of G is the set of elements which centralize all elements. *Center*

$$Z(G) = \{g \in G \mid gxg^{-1} = x, \forall x \in G\}$$

Alternatively,

$$Z(G) = \{g \in G \mid gx = xg, \forall x \in G\}.$$

Properties:

1. $Z(G) = G$ iff G is abelian.
2. $Z(G) = \cap_{x \in G} C_G(x)$.
3. $Z(G) \triangleleft G$.
4. We can also give conjugation as a group homomorphism[1]. [1] *$S(G)$ denotes set of bijections.*

$$\rho : G \to S(G)$$
$$\rho : G \to \mathrm{Aut}_{\mathsf{Sets}}(G)$$

Action is faithful $\Leftrightarrow$ trivial center (in general).

ρ is injective $\Leftrightarrow$ trivial center (only for conjugation).

Does it happen that $Z(G) = \{e\}$? Consider $A_5 < S_5$, the subgroup of even permutations. $Z(A_5) = \{e\}$.

Theorem 6.1 (Class formula for conjugation)**.** *Consider the action*

$$G \times G \to G$$

via conjugation. Denote by T the set of non-trivial orbit representatives, where Gx is non-trivial if $|Gx| > 1$. Notice that a trivial orbit looks like

$$G \cdot x = \{gxg^{-1} \mid g \in G\} = x,$$

when x commutes with everything, so $x \in Z(G)$.

$$|G| = \sum |Gx| = |Z(G)| + \sum_{x \in T} |Gx| = |Z(G)| + \sum_{x \in T} |G : C_G(x)|$$

6.1 p-groups and Sylow theorems

Definition (p-group)**.** A finite group G is called a p-**group**, p prime, if the order of G is a (positive) power of p. *p-group*

Remark 6.2 — p-groups are solvable.

Theorem 6.2. *Let G be a p-group. Then G has a non-trivial center.*

Proof. We'll prove that p divides $|Z(G)|$. This is what we want since $e \in Z(G) \Rightarrow |Z(G)| > 0$. Use the class formula for conjugation.

$$p^n = |G| = |Z(G)| + \sum_T |G : C_G(x)| = |Z(G)| + \sum_T \frac{|G|}{|C_G(x)|}$$

Since the identity is its own orbit,

$$1 < |Gx\| < |G| \Rightarrow 1 < \frac{|G|}{|C_G(X)|} < p^n.$$

Then since $|G| = p^n$ and the centralizers divide it, p divides each summand. Then p must divide $|Z(G)|$. ∎

Corollary 6.3. *If $|G| = p^2$, G is abelian. (homework)*

Remark 6.3 — Not true for p^3. For $p = 2$, consider Q_8, D_8.

Definition. Let G be any finite group. $H < G$ is a p-Sylow subgroup if

1. $|H| = p^n$,
2. and $(|G : H|, p) = 1$.

7 October 13, 2021

8 October 15, 2021

8.1 Sylow Theorems

Sylow p-subgroup

Definition (Sylow p-subgroup)**.** If $H < G$, we call it a **Sylow p-subgroup** of $|H| = p^n$ if

$$\left(\frac{|G|}{|H|}, p\right) = 1.$$

Theorem 8.1 (Sylow 1)**.** *If p divides $|G|$, then there exists a p-Sylow subgroup $H < G$.*

Theorem 8.2 (Sylow 2)**.** *The following are true.*

1. *Any 2 p-Sylow subgroups of G are conjugate.*
2. *If $Q < G$ is a Sylow p-subgroup, and $P < G$ is any p-subgroup, then there exists $g \in G$ such that*
$$gPg^{-1} \subset Q.$$
In other words, any p-subgroup embeds into a p-Sylow subgroup.

Theorem 8.3 (Sylow 3)**.** *Let N_p be the number of Sylow p-subgroups in G. Then*

1. $N_p \equiv 1 \pmod{p}$
2. *N_p divides $|G|$*
3. *$N_p = 1 \Leftrightarrow$ any Sylow p-subgroup is normal.*

Lemma 8.4. *Let $a = p^n m$, where $(m, p) = 1$. Then*

$$\left(\binom{a}{p^n}, p\right) = 1$$

Proof. Homework. ∎

Theorem 8.5. *p divides $|G|$ implies that there exists $P < G$ a p-Sylow subgroup.*

Proof. $|G| = p^n m$ where $(m, p) = 1$. Let

$$\Omega = \{X \subset G : |X| = p^n\}.$$

Consider the group action given by

$$G \times \Omega \to \Omega, \quad (g, x) \mapsto gX.$$

Then the class formula tells us

$$|\Omega| = \sum_X |G : G_X|,$$

summing over orbit representatives. The LHS, by the previous lemma, is not divisible by p. There exists $X \in \Omega$ such that p does not divide

$$G : G_X = \frac{|G|}{|G_x|}.$$

Then since p^n divides $|G|$, we must have p^n dividing $|G_x|$ (*). But also, G_X stabilizes X. $G_X = X$. Let $x \in X$.

$$G_X \cdot x = \{gx \mid g \in G_x\} \subset X$$

Then $|G_x| = |G_x \cdot x| \leq |X| = p^n$ (**). Then (*) and (**) give $|G_x| =; ^n$. ■

Sylow 2. If p, Q p Sylow in G, we want to find $g \in G$ such that $g^{-1}Pg = Q$. That is,

$$Pg = gQ$$

$$PgQ = gQ$$

Consider the action $G \times G/Q \to G/Q$ by left multiplication.

$$(x, gQ) - \mapsto xgQ$$

Restrict this action to $P < G$. $P \times G/Q \to G/Q$.

$$(x, gQ) - \mapsto xgQ$$

The class formula tells us

$$|G/Q| = \sum_{gQ} |P : \text{Stab}_P(gQ)|.$$

p does not divide $|G/Q|$ (Sylow).

$$|P : \text{Stab}_P(gQ) = \frac{|P|}{|\text{Stab}_P(gQ)|} = p^\alpha$$

for $0 \leq \alpha \leq n$ since $|P| = p^n$. There exists gQ such that $|P : \text{Stab}_P(gQ)| = 1$. But then

$$|P : gQ| = |P : \text{Stab}_P(gQ)| = 1$$

$$\Rightarrow PgQ = gQ \Rightarrow Pg \subset gQ \Rightarrow g^{-1}Pg \subset Q$$

P and Q are Sylow, so the containment must be equality: $g^{-1}Pg = Q$. Since we only used that P is a p-subgroup until the last couple steps, same argument gives

$$g^{-1}Pg \subset Q \Rightarrow P \subset gQg^{-1},$$

which is Sylow. We refer to Sylow 1 to get the existence of Q in the first place. ■

Sylow 3. 3. This is clear from Theorem 2.

2. The set of all Sylow subgroups, by Theorem 2, is

$$\{gPg^{-1} \mid P \text{ fixed Sylow}\}.$$

Consider the action $G \times 2^G \to 2^G$ by conjugation.

$$(g, X) \mapsto gXg^{-1}$$

Ω the orbit of P under conjugation. So $N_p = |\Omega| = |G \cdot P|$. Since $N_p = |G \cdot P|$, N_p divides $|G|$. In fact,

$$|G \cdot P| = |G : \text{Stab}_G(P)| = |G : \text{Norm}_G(P)| = \frac{|G|}{|\text{Norm}_G(P)|}$$

1. Left for Monday.

■

Remark 8.1 — If $P < G$ is Sylow, then for all $P < H < G$, we have that P is a p-Sylow subgroup in H.

9 October 18, 2021

Remark 9.1 — Observe that if $P < H < G$, and P is a p-sylow subgroup in G, then it is p-Sylow in H.

Proof. Finishing 1. in Sylow 3. Let P be a Sylow p-subgroup. Let $\mathcal{N}_G(P) = \text{Norm}_G(P)$. Consider the action via left multiplication of

$$P \times G/\mathcal{N}_G(P) \to G/\mathcal{N}_G(P).$$

Observe that since $|P| = p^n$,

$$(|G/\mathcal{N}_G(P)|, p) = 1.$$

Consider 2 types of orbits in $G/\mathcal{N}_G(P)$: trivial and non-trivial orbits (w.r.t. previously mentioned action). The size of any non-trivial orbit divides $|P| = p^n$. From our coprime observation, the class formula implies that there exists a trivial orbit. That is, there exists $g \in G$ such that

$$P(g\mathcal{N}_G(P)) = g\mathcal{N}_G(P).$$

Observe that

1. $g^{-1}Pg$ is a p-Sylow subgroup in $\mathcal{N}_G(P)$ because $g^{-1}Pg$ is p-sylow in G, and
2. $P \triangleleft \mathcal{N}_G(P)$.

These two observations imply that $g^{-1}Pg = P$, so $g \in \mathcal{N}_G(P)$.

$$g\mathcal{N}_G(P) = \mathcal{N}_G(P)$$

Any trivial orbit is $\mathcal{N}_G(P)$, so there is only 1. ■

Note that $|P| = p^n$, $|\mathcal{N}_G(P)| = p^n m$, $|G| = p^n k$, which gives us our coprimei observation in the above proof.

9.1 Products

Direct product

Definition (Direct product)**.** H, K groups. The **direct product** of H and K as

$$H \times K = \{(h, k) : h \in H, k \in K\}$$

equipped with the operation

$$(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2).$$

Units and inverses are inherited from H and K component-wise.

Example 9.1.

1. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{R} \simeq \mathbb{R}^*$ where
$$(\varepsilon, a) \mapsto \varepsilon e^a.$$
Inverse:
$$(\text{sign}(b), \ln|b|) \leftarrow b.$$
Note we take $\mathbb{Z}/2\mathbb{Z}$ to be additive or multiplicative in whichever way we need. We had before the short exact sequence
$$0 \to \mathbb{R} \to \mathbb{R}^* \to \mathbb{Z}/2\mathbb{Z} \to 1.$$
Note the relevance of this isomorphism.
2. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$. Note Chinese Remainder Theorem.
3. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \not\simeq \mathbb{Z}/4\mathbb{Z}$

Remark 9.2 — $|H \times K| = |H| \cdot |K|$, even with infinite groups.

Proposition 9.1. *If $G = H \times K$,*

1. *$H \simeq H \times \{e_K\} \triangleleft G$ and $K \simeq \{e_H\} \times K \triangleleft G$.*
2. *There exists a short exact sequence*
$$1 \to H \to^{i_H} H \times K \to^{\pi_k} K \to 1$$
with
$$h \mapsto (h, e_K), \quad (h, k) \mapsto k$$
which is "split," that is there exists $i_k : K \to H \times K$ such that $\pi_k \circ i_j = id_K$.

Question 9.1 — What are "split" sequences of finite groups.

Lemma 9.2. *Given, $A, B < G$, we can consider a map of sets $\mu : A \times B \to G$ given by $(a, b) \mapsto ab$.*

1. *μ is a homomorphism iff $ab = ba$ for all $a \in A, b \in B$.*
2. *μ is injective iff $A \cap B = e$*
3. *μ is surjective iff $AB = G$*

Then we have the following as a corollary.

Proposition 9.3. *If $A, B < G$, then $A \times B \simeq G$ iff*

1. *$A, B \triangleleft G$ (this is the one that usually fails),*
2. *$A \cap B = \{e\}$, and*
3. *$AB = G$.*

Torsion subgroup

Definition (Torsion subgroup)**.** A an abelian group, p prime.

$$A_{(p)} = \{a \in A \mid \exists i \in \mathbb{Z}_{\geq 0}, p^i a = 0\}$$

as the p**-torsion subgroup** in A. (additive notation, sum of p^i as)

Fact: If A is a finite abelian group, then

$$A \simeq \prod_{p \text{ prime}} A_{(p)}$$

(a finite product since there are finitely many p such that $A_{(p)}$ is non-trivial).

Example 9.2. $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

10 October 20, 2021

Consider the automorphism group of G

$$\mathrm{Aut}_{\mathrm{gr}}(G) = \{f : G \to G\},$$

which is a group with the operation of function compostion. This has an important subgroup

$$\mathrm{Inn}(G) = \{f_g : x \mapsto g^{-1}xg\},$$

the inner automorphisms of G.

Definition (Semi-direct product)**.** Coming soon. *Semi-direct product*

11 October 22, 2021

11.1 Semi-direct product

H acts on G by group automorphisms.

Given H, N groups, $H \to^{\varphi} \mathrm{Aut}_{\mathrm{gr}}(N)$ group homomorphism.

This allows us to construct semi-direct productstructure on N.

Construction:

$h \in H$, then $\varphi(h) : N \to N$. Notation $a \mapsto^h a$, $\varphi(h)(a)$.

Define multiplication on $N \times H$.

$$(a, h) \cdot (a', h') = (a({}^h a'), hh')$$

Identity is (e_N, e_H). Inverse $(a, h)^{-1}$ is $({}^{h^{-1}}a^{-1}, h^{-1})$. Checking inverse:

$$(a, h)({}^{h^{-1}}a^{-1}, h^{-1}) = (a\,{}^h({}^{h^{-1}}(a^{-1})), hh^{-1}) = (a({}^{hh^{-1}}a^{-1}), e) = (aa^{-1}, e) = e.$$

The resulting group is called the semi-direct product of H and N, denoted $N \rtimes H$ or $N \rtimes_{\varphi} H$, if we need to specify how H acts on N.

If $G = N \rtimes H$, we have the following observations.

1. $N, H < G$.
2. $N \triangleleft G$.
3. Conjugation:

$$(e, h)(a, e)(e, h)^{-1} = (e\,{}^h a, h)(e, h^{-1}) = ({}^h a, e)$$

Action of H on N becomes conjugatino in $N \rtimes H$.

Given $G = N \rtimes H$, there is a natural short exact sequence which splits.

$$1 \longrightarrow N \xrightarrow{i_N} N \rtimes H \xrightarrow{\pi} \frac{N \rtimes H}{N} \longrightarrow 1$$

$$\frac{N \rtimes H}{N} \simeq H, \qquad i_H : H \to N \rtimes H$$

$\pi \circ i_H = \mathrm{id}_H$.

Claim: $\frac{N \rtimes H}{N} \simeq H$. Check that π is a homomorphism in $N \rtimes H \to^{\pi} H$. $(a, h) \to h$. $\mathrm{Ker}\pi = N$.

Proposition 11.1. *Given $N, H < G$, say H acts on N by conjugation. TFAE.*

1. *$G \simeq N \rtimes H$ with $ah \leftarrow (a, h)$.*
2. *$N \triangleleft G$, $N \cap H = \{e\}$, and $NH = G$.*

3. *There exists* $\pi : G \to H$ *such that* $N = Ker\pi$, *and* $\pi \circ i_H = id_H$.
4. *There exists a short exact sequence*

$$1 \to N \to G \to_\pi H \to 1$$

which splits, that is, for $i_H : H \to G$, *then* $\pi \circ i_H = id_H$.

Example 11.1. S_3 has elements $\sigma(1\ 2\ 3)$ and $\tau(1\ 2)$ with orders 3 and 2 respectively.

$$(12)(123)(12) = (132)$$

Notice $\langle\sigma\rangle \simeq \mathbb{Z}/3\mathbb{Z}$ is fixed when conjugating by τ. $\mathbb{Z}/3\mathbb{Z} \triangleleft S_3$. $\mathbb{Z}/2\mathbb{Z} \cap \mathbb{Z}/3\mathbb{Z} = \{e\}$. τ, σ generate S_3. Then $S_3 \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ not direct since S_3 is not abelian. Same idea applies to $D_m \simeq \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, as S_3 is isomorphic to D_3.

Proof. (1) to (2) is easy. Equivalence of (3) and (4) comes from terminology. From (1) to (3),

$$G = N \rtimes H \to H$$

where $H \to \frac{N \rtimes H}{N} \simeq H$, $i_H : H \to N \rtimes H$, and $\bar{i} : N \rtimes H \to H$. $(a, h) \to (e, h)$ and $(e, h) \leftarrow h$. For (2) to (1), $N, H < G, N \triangleleft G$. H acts on N by conjugation.

$$N \rtimes H \to^f G \quad (a, h) \to ah$$

Need to check

1. f is a homomorphism.

$$(a, h)(a', h) \in N \rtimes H$$
$$(a, h)(a', h') = (a\,{}^h(a'), hh')$$
$$f((a\,{}^h(a'), hh')) = a\,{}^h a^{-1} hh' = a(ha'h^{-1})hh' = aha'h'$$
$$f((a, h))f((a', h')) = aha'h'$$

2. f is injective. Suppose $f(a, h) = f(a', h')$.

$$(a')^{-1}a = h'h^{-1} = e$$

since $N \cap H = \{e\}$, so $ah = a'h'$.

3. f is surjective. $N \rtimes H \to G$. $(a, h) \to ah$, and $NH = G$.

Leave (3) to (2) as an exercise. ∎

12 October 25, 2021

12.1 *Filtrations, solvable and nilpotent groups*

Filtration

Definition (Filtration)**.** A **decreasing filtration** of group G is a tower of subgroups

$$\ldots < G_2 < G_1 < G_0 < G$$

where $G_i < G$ is a subgroup. An **increasing filtration** is

$$e = G_0 < G_1 < \ldots.$$

A **finite filtration** has finitely many terms.

$$e = G_n < \ldots < G_1 < G_0 = G$$

A **normal filtration** has normality between each consecutive subgroup, $G_i \triangleleft G_{i-1}$. A normal filtration is abelian if for all i, G_{i-1}/G_i is abelian.

Remark 12.1 — In normal filtrations, it's not necessarily true that $G_i \triangleleft G$.

Example 12.1.

1. $G = N \rtimes H$ gives
$$e \triangleleft N \triangleleft G$$
a normal filtration. This didn't have to be semi-direct product; we could have used any G with normal subgroup N.
2. The alternating group (even permutations) $A_n < S_n$.
$$e \triangleleft A_n \triangleleft S_n$$

Lemma 12.1. *If G (finite) has a (finite) normal abelian filtration, then it has (finite) normal filtration with cyclic factors. In other words, any abelian filtration can be refined to a cyclic filtration.*

Proof. Let

$$e < \ldots G_2 < G_1 < G_0 = G$$

be an abelian filtration.

$$\ldots \triangleleft G_i \triangleleft G_{i-1} \triangleleft \ldots$$

We know G_{i-1}/G_i is abelian. We claim that any finite abelian group A has a finite filtration with cyclic factors. This is shown by induction (on $|A|$). Let non-identity $a \in A$. $\langle a \rangle < A$ is cyclic. Either $\langle a \rangle = A$ and $e < A$ works, or $A' = A/\langle A \rangle$ has a smaller order, and therefore has a filtration with cyclic factors by induction.

$$e \triangleleft \ldots \triangleleft A_2' \triangleleft A_1' \triangleleft A'$$

can be lifted to

$$\langle a \rangle \triangleleft \ldots \triangleleft A_2 \triangleleft A_1 \triangleleft A$$

where A_i are subgroups of A corresponding to $A_i' \triangleleft A'$ (third isomorphism theorem). This ends the claim. Then we have the following lifting

$$G_i \triangleleft \ldots \triangleleft G_{i-1}^2 \triangleleft G_{i-1}^1 \triangleleft G_{i-1}$$

from

$$e \triangleleft \ldots \overline{G}_{i-1}^2 \triangleleft \overline{G}_{i-1}^1 \triangleleft G_{i-1}/G_i.$$

In summary we just lifted the filtration from e to G_{i-1}/G_i to the filtration of G_i to G_{i-1}. By the third isomorphism theorem again,

$$G_{i-1}^j \triangleleft G_{i-1}^{j-1} \quad \text{and} \quad G_{i-1}^{j-1}/G_{i-1}^j \simeq \overline{G}_{i-1}^{j-1}/\overline{G}_{i-1}^j \quad \text{which is cyclic.}$$

■

Note that the terms filtration, tower, and series are all interchangeable.

Definition. The **commutator (derived) subgroup** of G is

$$[G, G] = \langle [x, y] : x, y \in G \rangle$$

> Remark 12.2 — The set of all commutators itself is not necessarily a subgroup, so we take the subgroup generated by all commutators in the definition above.

Lemma 12.2. *Suppose we have $H, K \triangleleft G$.*

$$[H, K] = \langle [h, k] : h \in H, k \in K \rangle \triangleleft G$$

Proof. Notice we can write

$$ghkh^{-1}k^{-1}g^{-1} = (ghg^{-1})(gkg^{-1})(gh^{-1}g^{-1})(gk^{-1}g^{-1}).$$

■

Corollary 12.3. *We always have $[G, G] \triangleleft G$.*

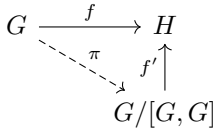
Proposition 12.4. *1. $G/[G, G]$ is abelian. This quotient is called the **abelianization** of G (largest abelian quotient).*

2. We can write

$$[G, G] = \bigcap_{N \triangleleft G} N$$

where G/N is abelian, formalizing the idea that $G/[G, G]$ is the largest abelian quotient of G.

3. *Universal property. For any $f : G \to H$ with H abelian, there exists unique $f' : G/[G,G] \to H$ such that $f = f' \circ \pi$.*



13 October 29, 2021

Definition (Perfect)**.** G is **perfect** if $[G, G] = G$. *Perfect*

Definition (Derived series)**.** The **derived series** of G is *Derived series*

$$G^{(0)} = G, G^{(1)} = [G, G], \ldots, G^{(i+1)} = [G^{(i)}, G^{(i)}]$$

where

$$\ldots \triangleleft G^{(1)} \triangleleft G^{(0)} = G$$

Remark 13.1 — Observe that each $G^{(i)} \triangleleft G$ by last time's lemma.

$$G^{(i)} \triangleleft G \Rightarrow [G^{(i)}, G^{(i)}] \triangleleft G$$

Example 13.1.

1. In S_4,
$$e \triangleleft V_4 \triangleleft A_4 \triangleleft S_4,$$
where $V_4 = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. Quotient between S_4 and A_4 is $\mathbb{Z}/2\mathbb{Z}$ and quotient between A_4 and V_4 is $\mathbb{Z}/3\mathbb{Z}$.
2. For $n \geq 5$,
$$[S_n, S_n] = A_n, \quad [A_n, A_n] = A_n$$

Proposition 13.1. *TFAE.*

1. *There exists a finite normal series with abelian factors.*
$$e = G_n \ldots \triangleleft G_1 \triangleleft G_0 = G$$
2. *There exists a finite normal series with abelian factors such that $G_i \triangleleft G$.*
3. *The derived series for G terminates at $G^{(m)} = e$ after finitely many steps.*

Proof. (3) to (2) to (1) is immediate from the strength of the statements. We need only consider (1) to (3). Let

$$e = G_n \triangleleft G_{n-1} \triangleleft \ldots \triangleleft G_0 = G$$

be some normal series with G_i/G_{i+1} abelian. Recall notation for derived series. We claim that $G^{(i)} < G_i$, which is sufficient to prove the desired statement (set $i = n$). We proceed by induction. For $i = 0$, $G^{(0)} = G_0 = G$. For the induction step $i \mapsto i + 1$, we know $G^{(i)} < G_i$, and $G^{(i+1)} = [G^{(i)}, G^{(i)}] < [G_i, G_i]$. $G_{i+1} \triangleleft G_i$ and G_i/G_{i+1} is abelian. This implies that $G_{i+1} > [G_i, G_i]$. So

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] < [G_i, G_i] < G_{i+1},$$

and we conclude $G^{(n)} < G_n = e$, that is the derived series terminates. ■

Definition (Solvable)**.** A group G satisfying the equivalent conditions of the proposition is called **solvable**. *Solvable*

Example 13.2. S_4 we saw earlier. Any abelian group is trivially solvable.

13.1 Central series and nilpotent groups

Definition (Central)**.** $H < G$ is **central** if $H < Z(G)$. *Central*

Remark 13.2 — H central is trivially normal. Alternatively, $[H, G] = e$.

Lemma 13.2. *$H < K < G$. TFAE.*

1. *$H \triangleleft G$ and $K/H < Z(G/H)$.*
2. *$[K, G] \subset H$.*

Proof. (1) to (2). $K/H < Z(G/H)$ implies $[K/H, G/H] = e$. Then invoke the third isomorphism theorem. (2) to (1). Observation. Forall $H, K < G$, $[H, K] = [K, H]$. Then $[h, k]^{-1} \in [K, H]$. (2) to (1). We want to show $H \triangleleft G$. For $g \in G, h \in H$,

$$ghg^{-1} = ghg^{-1}h^{-1}h = [g, h]h \in [G, H]H \subset [G, K]H = [K, G]H \subset H.$$

Let $k \in K, g \in G$. Consider kH. Need to show $kHgH = gHkH$. Since $[, g] \in H$, we can write

$$kgH = gkH = gHkH$$

■

Definition (Central)**.** A descending series of G is called **central** if one of the following equivalent conditions holds. *Central*

1. $G_i \triangleleft G, G_i/G_{i+1} < Z(G/G_{i+1})$
2. $[G_i, G] < G_{i+1}$

Remark 13.3 — We can define an ascending series of G to be central analogously.

Definition. The **descending central series** for G is

$$\ldots \Gamma_2 < \Gamma_1 < \Gamma_0 = G$$

where $\Gamma_i = [\Gamma_{i-1}, G]$. Note

$$\Gamma_1 = [\Gamma_0, G] = [G, G]$$

while

$$\Gamma_2 = [\Gamma_1, G] > [\Gamma_1, \Gamma_1]$$
$$[[G, G], G] > [[G, G], [G, G]]$$

Definition. The ascending central series for G is

$$e = Z_0 < Z_1 < Z_2 < \dots$$

where $Z_1 = Z(G)$ and $Z_i/Z_{i-1} = Z(G/Z_{i-1})$.

Remark 13.4 — Definition makes sense because of the third isomorphism theorem. We construct Z_i recursively. Say we constructed

$$e = Z_0 < Z_1 < \dots < Z_{i-1} < G$$

Let $\overline{Z}_i = Z(G/Z_{i-1})$ and lift to $Z_{i-1} < Z_i$ (third isomorphism theorem).

Proposition 13.3. *TFAE.*

1. *There exists a finite central series for G.*
2. *The descending central series terminates at e.*
3. *The ascending central series terminates at G.*

14 November 1, 2021

Nilpotent

Definition (Nilpotent)**.** G is **nilpotent** if it satisfies conditions of the previous proposition.

Remark 14.1 — Any solvable group is nilpotent. Reverse is not true (consider S_3).

$$e \triangleleft [S_3, S_3] \triangleleft S_3$$

$[S_3, S_3] \simeq A_3 \simeq \mathbb{Z}/3\mathbb{Z}$.

$$e \triangleleft \mathbb{Z}/e\mathbb{Z} = \langle r \rangle \simeq \triangleleft D_3 = \langle r, s \rangle$$

On the other hand,

$$[A_3, S_3] = A_3 \triangleleft A_3 = [S_3, S_3] \triangleleft S_3,$$

so not nilpotent.

Proposition 14.1. *Let G be a p-group. Then G is nilpotent.*

Proof. Induction on order. Base case: $|G| = p$ requires G to be abelian, so it is nilpotent. Induction step: G is a p-group, so it has non-trivial center. Then by induction, $G/Z(G)$ has a finite central series. We lift by the third isomorphism theorem.

$$e \triangleleft Z(G) \triangleleft \ldots \triangleleft G$$

■

Theorem 14.2 (Structure of finite nilpotent groups)**.** *If G is finite nilpotent, then $G = P_1 \times P_2 \times \ldots P_n$, where P_i is a Sylow p_i-subgroup.*

Lemma 14.3. *If $H < G$ is a proper subgroup, then H is also a proper subgroup of its normalizer $N_G(H)$.*

Proof. Let

$$e \triangleleft G_{n-1} \triangleleft G_{n-2} \triangleleft \ldots \triangleleft G_2 \triangleleft G_1 \triangleleft G_0 = G$$

be a descending central series. There exists unique i (with $0 \leq i \leq n$) such hat $G_i < H$ but $G_{i-1} \not< H$. Warning: we cannot necessarily have $G_i < H < G_{i-1}$.

$$e \triangleleft \mathbb{Z}/3\mathbb{Z} \triangleleft \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$e \triangleleft \mathbb{Z}/2\mathbb{Z} \triangleleft \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Let $g \in G_{i-1} \setminus H$. Since the series is central, $G_{i-1}/G < Z(G/G_i)$. $\overline{g} = g \mod G_i$. $\overline{g}$ centralizes $H/G_i < G/G_i$, that is,

$$\overline{g}\overline{h}\overline{g}^{-1} \in H/G_i$$

for all $h \in H$. Then $ghg^{-1} \in H$ which implies $g \in N_G(H)$.

$$gG_ihG_ig^{-1}G_i \subset H$$

$$ghg^{-1}G_i \subset H$$

■

Proposition 14.4. *G_1, G_2 groups, $H \triangleleft G_1, K \triangleleft G_2$.*

1. $H \times K \triangleleft G_1 \times G_2$
2. $(G_1 \times G_2)/H \times K \simeq (G_1/H) \times (G_2/K)$
3. $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$

Proof. Isomorphism theorems. ■

Corollary 14.5. 1. *G_1, G_2 nilpotent implies $G_1 \times G_2$ nilpotent*

2. *$G_1, \ldots G_n$ nilpotent implies $G_1 \times \ldots \times G_n$ nilpotent.*

Proposition 14.6. *Let P be a Sylow-p subgroup in G nilpotent. Then $N_G(N_G(P)) = N_G(P)$*

Proof. HW, do not use structure theorem. ■

Theorem 14.7. *Let G be a finite group. G is nilpotent iff G is a direct product of all its Sylow subgroups.*

Proof. ($\Rightarrow$) P_i nilpotent as p_i-groups implies $P_1 \times \ldots \times P_n$ is nilpotent. ($\Leftarrow$) $|P_i| = p_i^{\alpha_i}$. Claim: let $P < G$ be any p-Sylow subgroup. Then $P \triangleleft G$. Proof of claim:

- G nilpotent, $P \leq G$ implies $P < N_G(P) < G$ (proper subgroups). By the previous proposition, $N_G(N_G(P)) = N_G(P)$, and lemma tells us $N_G(P) < G$ (strict) implies $N_G(N_G(P))$. Therefore $N_G(P) = G$ implies $P \triangleleft G$.

■

15 November 3, 2021

Continued. Now let $|G| = \prod p_i^{a_i}$. Let P_i be the Sylow p_i-subgroup. Then

- $P_i \cap P_j = e$
- $P_i \triangleleft G$
- $P_1 P_2 \dots P_n = G$ (since if one is normal, set product is a subgroup, then we just enumerate elements)

Therefore by the Lemma on characterizing direct product, $P_1 \times \dots \times P_n \simeq G$. ■

15.0.1 Jordan Holder Theorem

Simple

Definition (Simple)**.** G is **simple** if it does not have proper non-trivial normal subgroups.

Composition series

Definition (Composition series)**.** The series

$$e = G_n < \dots < G_1 < G_0 = G$$

is a finite normal series. It is a **composition series** if G_i/G_{i+1} is simple for all i.

Proposition 15.1. *1. Any finite abelian group has a composition series*

2. If G has a finite normal series with abelian quotients, then G has a composition series.

Proof. Simple abelian groups: $\mathbb{Z}/p\mathbb{Z}$.

1. By induction, for example.
2. If we have
$$e = G_n \triangleleft G_{n-1} \triangleleft \dots \triangleleft G_2 \triangleleft G_1 \triangleleft G,$$
since G_i/G_{i+1} is abelian, it has composition series by (1).
$$e = \overline{G}_i^{n_i} \triangleleft \overline{G}_i^{n_i - 1} \triangleleft \dots \triangleleft \overline{G}_i^2 \triangleleft \overline{G}_i^1 \triangleleft G_i/G_{i+1}$$
We can lift (by third isomorphism) to
$$e = G_i^{n_i} \triangleleft G_i^{n_i - 1} \triangleleft \dots \triangleleft G_i^2 \triangleleft G_i^1 \triangleleft G_i$$

■

Remark 15.1 — Composition series is not unique.

$$e \triangleleft \mathbb{Z}/2\mathbb{Z} \triangleleft \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \quad \text{and} \quad e \triangleleft \mathbb{Z}/2\mathbb{Z} \triangleleft \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

However, the set of intermediate quotients are the same.

Equivalent

Definition (Equivalent)**.** Two composition series are **equivalent** if they have the same length and there is one-to-one correspondence between the intermediate quotients of the series.

Theorem 15.2 (Jordan-Holder)**.** *Any 2 composition series for G are equivalent.*

Theorem 15.3 (Schreier)**.** *For group G, any two finite normal series have equivalent refinements.*

$$e = G_n \triangleleft \ldots \triangleleft G_2 \triangleleft G_1 \triangleleft G$$
$$e = G_n \triangleleft \ldots \triangleleft G_{i+1} \triangleleft G_i^{n_j} \triangleleft G_i^{n_j - 1} \triangleleft \ldots \triangleleft G_i^1 \triangleleft G_i \triangleleft \ldots \triangleleft G_2 \triangleleft G_1 \triangleleft G$$

The bottom series is a refinement of the top.

Sketch.

$$e = G_n \triangleleft \ldots G_1 \triangleleft G$$
$$e = H_m \triangleleft \ldots H_1 \triangleleft G$$

Consider $G_{i+1} \triangleleft G$. Take intersections.

$$e = G_i \cap e \triangleleft G_i \cap H_{m-1} \triangleleft \ldots G_i \cap H_2 \triangleleft G_i \cap H_1 \triangleleft G_i$$

Multiply by G_{i+1}.

$$e = G_{i+1} \triangleleft G_{i+1}(G_i \cap H_{m-1}) \triangleleft \ldots G_{i+1}(G_i \cap H_2) \triangleleft G_{i+1}(G_i \cap H_1) \triangleleft G_i$$

■

16 November 5, 2021

Lemma 16.1 (Zassenhaus). *Given $G_2 \triangleleft G_1 < G$ and $H_2 \triangleleft H_1 < G$,*

1. *$G_2(G_1 \cap H_2) \triangleleft G_2(G_1 \cap H_1)$,*
2. *$H_2(G_2 \cap H_1) \triangleleft H_2(G_1 \cap H_1)$, and*
3. *from the second isomorphism theorem,*

$$\frac{G_2(G_1 \cap H_1)}{G_2(G_1 \cap H_2)} \simeq \frac{H_2(G_1 \cap H_1)}{H_2(G_2 \cap H_1)}$$

Proof. (maybe later) We'll show

$$\frac{G_2(G_1 \cap H_1)}{G_2(G_1 \cap H_2)} \simeq \frac{(G_1 \cap H_1)}{(G_2 \cap H_1)(G_1 \cap H_2)}$$

■

Theorem 16.2 (Shreier). *Any two finite normal series of G have equivalent refinements.*

Proof. Take two finite normal series.

$$e = G_n \triangleleft \ldots \triangleleft G_{i+1} \triangleleft G_i \triangleleft \ldots \triangleleft G_1 \triangleleft G$$

$$e = H_n \triangleleft \ldots \triangleleft H_{i+1} \triangleleft H_i \triangleleft \ldots \triangleleft H_1 \triangleleft H$$

Refine by intersecting the entire H series with G_i.

$$e = G_i \cap H_m \triangleleft \ldots \triangleleft G_i \cap H_2 \triangleleft G_i \cap H_1 \triangleleft G_i$$

Then multiply by G_{i+1}.

$$G_{i+1} = G_{i+1}(G_i \cap H_m) \triangleleft \ldots \triangleleft G_{i+1}(G_i \cap H_j) \triangleleft \ldots \triangleleft G_{i+1}G_i = G_i$$

Define

$$G_{i,j} = G_{i+1}(G_i \cap H_j) \quad \text{and} \quad H_{ji} = H_{j+1}(H_j \cap G_i)$$

We claim that $G_{i,j}$ is a refinement of the G_i series.

$$\ldots \triangleleft G_{i+1} \triangleleft G_{i,j} \triangleleft \ldots \triangleleft G_i \triangleleft G_{0,m} \triangleleft \ldots \triangleleft G_{0,1} \triangleleft G_0 = G$$

This is because $G_{i,j} \triangleleft G_{i,j-1}$. This is Zassenhaus lemma.

$$G_{i,j} \triangleleft G_{i,j-1}$$

$$G_{i+1}(G_i \cap H_{j+1}) \triangleleft G_{i+1}(G_i \cap H_j)$$

$$G_{i+1} \triangleleft G_i \quad H_{j+1} \triangleleft H_j$$

Equivalence between the refined H and refined G series.

$$H_{j,i+1} \triangleleft H_{j,i}$$

$$H_{j+1}(H_j \cap G_{i+1}) \triangleleft H_{j+1}(H_j \cap G_i)$$

By Zassenhaus again,

$$\frac{G_{i,j}}{G_{i,j+1}} = \frac{G_{i+1}(G_i \cap H_j)}{G_{i+1}(G_i \cap H_{i+1})} \quad \text{and} \quad \frac{H_{i,j}}{H_{j,i+1}} = \frac{H_{j+1}(H_j \cap G_i)}{H_{j+1}(H_j \cap G_{i+1})}$$

■

Corollary 16.3. *Compositions series are unique up to equivalence.*

Proof. Compositions series are their own refinements, i.e. no further refinement is possible. Apply Shreier. ■

Remark 16.1 — Existence. If G is finite, then either G is simple or $e \triangleleft N \triangleleft G$. If N has a composition series and G/N has a composition series, then G does (third isomorphism theorem and lift).

16.1 Free groups, generators, & relations

Given a set X, construct set X^{-1} where there is a bijection between $X \leftrightarrow X^{-1}$. Let $e \notin X, X^{-1}$. Consider $X \mapsto F(X)$, the free group on X. A word is a sequence of letters where a letter is an element in X, X^{-1}, or e. We treat e as an empty word. A word looks like

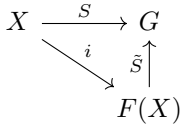
$$a_1 a_2 \dots a_n \quad a_i \in X \cup X^{-1} \cup \{e\}.$$

Definition. 2 words are **elementary equivalent** if we can obtain one from the other by adding or deleting xx^{-1} or $x^{-1}x$ or e. $w \sim w'$ if there is a sequence of elementary equivalences between them.

Definition (Free group)**.** $F(X)$ is a set of equivalence class of words, with concatenation as its operation. *Free group*

Claim: $F(X)$ is a group.

Proposition 16.4. *Universal property: X a set, G a group. For all $S : X \to G$, there exists a unique map*



There exists a unique group homomorphism $F(X) \to^{\tilde{S}} G$ such that the diagram commutes, where $X \to^{i} F(x)$ with $x \mapsto i(x)$.

17 November 8, 2021

Remark 17.1 — F sends sets to groups (functor).

Definition. For W set of words on $X \coprod X^{-1}$ ($W \subset F(X)$),

1. u, v words are W-elementary equivalent if we can get from u to v by
   (a) adding or deleting a word $w \in W$, or
   (b) adding or deleting $xx^{-1}, x^{-1}x, e$, and
2. $u \sim_W v$ if we can get from u to v via a finite sequence of W-elementary equivalences.

Proposition 17.1. *1. $\sim_W$ is an equivalence relation on words.*

2. $ev \sim_W ve$.

3. $u_1 \sim_W v_1$ and $u_2 \sim_W v_2$ implies $u_1u_2 \sim_W v_1v_2$.

4. $(uv)s \sim_W u(vs)$ (thinking about equivalence classes, not just direct equality). Alternatively, $[uv]s \sim_W u[vs]$.

Proof. Clear (exercise?). ■

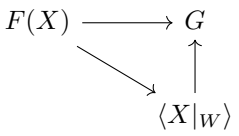
$\langle X|_W \rangle$ is the set of W-equivalence classes of words on $X \coprod X^{-1}$ with group operation of concatenation. This is the group with **generators** X and **relations** W.

Proposition 17.2. *For any G, there exists $F(X)$ and $F(X) \twoheadrightarrow G$ surjective homomorphism.*

Proof. $X = \{s_g\}_{g \in G}$, choose F to send $s_g \mapsto g$. ■

Proposition 17.3. *Let $\{g_i\}_{i \in I}$ be a set of a generators of G, $X = \{x_i\}_{i \in I}$, and $W \subseteq F(X)$, a set of words on X. Assume that for all $u = x_{i_1}^{\pm 1} \dots x_{i_n}^{\pm 1} \in W$, we have $g_{i_1}^{\pm 1} \dots g_{i_n}^{\pm 1} = e$. Then there exists group epimorphism $\langle X|_W \rangle \twoheadrightarrow G$ which sends $x_i \mapsto g_i$.*

Proof. We can factor.



■

Remark 17.2 — $F(X) \twoheadrightarrow \langle X|_W \rangle$. The kernel is

$$\text{Ker} = \bigcap_{N \triangleleft F(X), W \subseteq N} N$$

17.0.1 Presenting G with generators and relations

$$\text{Ker}\pi = N \hookrightarrow F(X) \twoheadrightarrow^{\pi} G.$$

Could choose $W = N$ (in practice, never happens).

Reduced words (no subwords of W). $F(X)$. Think about the English words rapport, which can be written as rap[2]ort.

[2] *This should also be treated as an exponent.*

$$u = x_1^{a_1} \dots x_n^{a_n}, \quad a_i \in \mathbb{Z} \setminus \{0\}$$

with $x_i \neq x_{i+1}$ and $x_i \neq x_{i+1}^{-1}$.

Example 17.1.

1. Integers.
$$\mathbb{Z} = \{x^-, ex^n \mid n \in \mathbb{Z}, n \neq 0\}$$
2. Direct product of integers.
$$\mathbb{Z} \times \mathbb{Z} = \langle x, y | xyx^{-1}y^{-1} = e \rangle$$
$$= \langle x, y | x^{-1}y^{-1}xy = e \rangle$$
$$= \langle x, y | xy = yx \rangle$$
3. Quotient.
$$\mathbb{Z}/n\mathbb{Z} = \langle x | x^n = e \rangle$$
4. Dihedral/symmetric group of order 6.
$$G = \langle x, y | x^2 = y^2 = e, (xy)^3 = e \rangle \simeq D_3 \simeq S_3$$
is a different presentation from what we are used to:
$$D_3 = \langle r, s | r^3 = s^2 = e, srsr = e \rangle$$

18 November 12, 2021

18.1 *Free and amalgamated products*

Free product

Definition (Free product)**.** Given $G_1 = \langle X_1|_{W_1}\rangle$ and $G_2 = \langle X_2|_{W_2}\rangle$, we define

$$G_1 * G_2 = \left\langle X_1 \coprod X_2|_{W_1 \cup W_2} \right\rangle.$$

to be the **free product** of G_1 and G_2.

Remark 18.1 — This is much larger than the direct product, since in $G_1 \times G_2$ we add commutative relations.

Example 18.1. Consider $\mathbb{Z} = \langle x\rangle$ and $\mathbb{Z} = \langle y\rangle$. We have

$$\mathbb{Z} \times \mathbb{Z} = \langle x, y|_{xyx^{-1}y^{-1}=e}\rangle$$

and

$$\mathbb{Z} * \mathbb{Z} = \langle x, y\rangle = F(\{x, y\}).$$

In the free product, the element $xyx^2y^2x^3y^3 \neq x^6y^6$.

Example 18.2. Consider $\mathbb{Z}/n\mathbb{Z} * \mathbb{Z}/n\mathbb{Z}$, where x, y generate each of the two copies of these cyclic groups. Then

$$\mathbb{Z}/n\mathbb{Z} * \mathbb{Z}/n\mathbb{Z} = \langle x, y|_{x^n=y^n=e}\rangle.$$

This is an infinite group, whose elements are written as

$$x^{a_1}y^{b_1}\dots x^{a_i}y^{b_i}$$

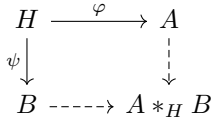
where $0 \leq a_k, b_k < n$.

Amalgamated product

Definition (Amalgamated product)**.** Given $A = \langle X_A|_{W_A}\rangle$, $B = \langle X_B|_{W_B}\rangle$, $H = \langle X_H|_{W_H}\rangle$ and homomorphisms $\varphi : H \to A, \psi : H \to B$, we define

$$A *_H B = \left\langle X_A \coprod X_B|W_A, W_B, \varphi(x)\psi^{-1}(x) = e\ \forall x \in H \right\rangle.$$

to be the **amalgamated product** of A and B.



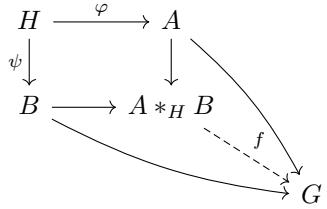
Remark 18.2 — $N \triangleleft A * B$ the minimal normal subgroup containing $\varphi(x)\psi^{-1}(x)$ over all $x \in X_H$. Then

$$\frac{A * B}{N} \simeq A *_H B$$

Remark 18.3 — Taking $H = \{e\}$, we see that the free product is a trivial amalgamated product.

Universal property.

Proposition 18.1. *Assume we have a commutative diagram.*

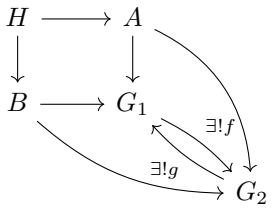


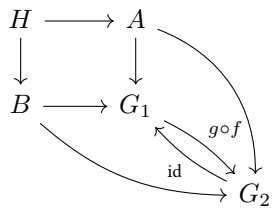
There exists a unique group homomorphism $f : A *_H B \to G$ such that the diagram commutes. In other words, there is a one to one correspondence between such commutative diagrams and $\{A *_H B \to G\}$. General nonsense: free product is coproduct final object.

Proof. Basically tautological. Exercise. ■

Corollary 18.2. *$A *_H B$ is uniquely defined up to a unique isomorphism.*

Proof. Suppose $G_1 = A *_H B$ and $G_2 = A *_H B$ constructed with different presentations for A, B, H.





By uniqueness of the universal property, $g \circ f = \mathrm{id}_{G_1}$. Similarly $f \circ g = \mathrm{id}_{G_2}$. Therefore, f, g are isomorphisms (and we already know uniqueness from universal property). ■

19 November 17, 2021

19.1 Rings

Ring

Definition (Ring)**.** A **ring** R is a set equipped with operations $(+, \times)$.

1. $(R, +)$ (where $0 \in \mathbb{R}$) is an abelian group.
2. $\times$ is associative.
3. It satisfies the distributive property.

$$a(b+c) = ab + bc$$
$$(b+c)a = ba + ca$$

4. $1 \in R$ is a two sided unit for $\times$.

$$1 \cdot a = a \cdot 1 = a \quad \forall\, a \in \mathbb{R}, a \neq 0$$

Remark 19.1 — Sometimes (4) is omitted. For us, rings will always have units.

Commutative

Definition (Commuative)**.** A ring R is **commutative** if $ab = ba$ for all $a, b \in R$.

Example 19.1. $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ are examples of rings (with the expected operations). Fields $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ are (fields and therefore trivially) rings. Polynomial rings are more interesting examples: $R[x], R[x_1, \ldots, x_n], \mathbb{R}(x)$. Power series: $R[[x]]$.

Field

Definition (Field)**.** F is a **field** if it is a commutative ring such that any non-zero $a \in F$ has an inverse ($aa^{-1} = a^{-1}a = 1$).

Division ring

Definition (Division ring)**.** D is a **division ring** if it is a is a ring (typically non-commutative, otherwise it's a field) such that all non-zero $a \in D$ is invertible.

Example 19.2. $\mathbb{R}$, $\mathbb{C}$, Q (quaternions).

Prime field. F a field,

$$F_0 = \bigcap_{K \subset F} K$$

where K are subfields. F_0 is a prime sub-field.

Ring homomorphism

Definition (Ring homomorphism)**.** For rings R, S, $f : R \to S$ is a **ring homomorphism** if

1. f is a homomorphism of abelian groups $(R, +)$ and $(S, +)$.
2. $f(ab) = f(a)f(b)$.

Characteristic

Definition (Characteristic)**.** For F a ring, $\varphi : \mathbb{Z} \to F$ is a ring homomorphism that sends 1 to 1. There exists minimal $p \in \text{Ker}\varphi$. If $\text{Ker}\varphi = 0$, φ is injective, and $\text{char}F = 0$. If p is the minimal prime in $\text{Ker}\varphi$ ($\varphi(p) = 0$), then $p = \text{char}F$.

We say R is a commutative ring (with 1) unless otherwise specified.

Definition. $I \subset R$ an abelian subgroup (with respect to $+$) is an **ideal** if for all $a \in I$ and $b \in R$, $ab \in I$.

Remark 19.2 — If R is not commutative, we can define left, right, and 2-sided ideals.

Kernel

Definition (Kernel)**.** $f : R \to S$ is a ring homomorphism. The **kernel** of f (which lives in R) is

$$\text{Ker}f = \{a \in R : f(a) = 0\},$$

and the **image** of f (which lives in S) is

$$\text{Im}f = \{b \in S : b = f(a), a \in R\}.$$

Proposition 19.1. *For $f : R \to S$ a ring homomorphism, $\text{Ker}f$ is an ideal in R.*

Proof. $a \in \text{Ker}f$, $b \in R$ implies

$$f(ab) = f(a)f(b) = 0$$

which means $ab \in \text{Ker}f$. ∎

Remark 19.3 — The image of f is not an ideal. Ideals sort of act for rings as normal subgroups do for groups.

Remark 19.4 — 0 is in any ideal.

Example 19.3.
1. Consider the ring of integers $\mathbb{Z}$. $n\mathbb{Z} = (n) = \{a \in \mathbb{Z} : n \mid a\}$ is an ideal.
2. In the polynomial ring $F[x]$, $f(x)F[x] = \{g(x) \in F[x] : f(x) \mid g(x)\}$ is an ideal. ($\mathbb{R}[x]$ our most typical example).

Generate

Definition (Generate)**.** $I \subset R$ an ideal is **generated** by $\{a_1, \ldots, a_n\}$ if for all $a \in I$, we can write

$$a = \sum_{i=1}^{n} b_i a_i.$$

We use the notation

$$I = (a_1, \ldots, a_n).$$

Principal ideal

Definition (Principal ideal)**.** A **principal ideal** I is generated by 1 element. $I = (a)$.

Reminder: rings R are commutative.

Factor Ring

Definition (Factor Ring)**.** Construction: For $I \subset R$, $a \sim_I b \Leftrightarrow a - b \in I$ is an equivalence relation. It also behaves well with respect to our operations. R/I, a **factor ring** is "the ring of equivalence classes" with respect to $\sim_I$.

Example 19.4. (n) is an ideal of $\mathbb{Z}$. $\mathbb{Z}/n\mathbb{Z}$, the integers modulo n, is a factor ring.

Definition. $f : R \to S$ is

1. injective if $f(r) = 0 \Rightarrow r = 0$,
2. surjective if for all $b \in S$, there exists $a \in R$ such that $b = f(a)$, and
3. an isomorphism if it is injective and surjective or equivalently, has an inverse.

Proposition 19.2. *f a ring homomorphism.*

1. *f is injective iff $Ker f = 0$.*
2. *f is surjective iff $Im f = S$.*

Theorem 19.3. *$I \subset R$ an ideal. There exists a 1-to-1 correspondence between ideals in R/I and ideals $J \subset R$ such that $I \subset J \subset R$.*

Zero-divisor

Definition (Zero-divisor)**.** $a \in \mathbb{R}$ is a **zero-divisor** if there exists non-zero $b \in R$ such that $ab = 0$.

Integral domain

Definition (Integral domain)**.** R is an **(integral) domain** if R does not have non-trivial zero divisors or equivalently, the only zero-divisor is zero itself.

Our fields will always contain two elements.

Example 19.5. $\mathbb{Z}$ is a domain. $F[x]$ is a domain. Any field is a domain. Note that $\mathbb{Z}/6\mathbb{Z}$ is not a domain, as $3 \cdot 2 = 6$. In fact, $\mathbb{Z}/n\mathbb{Z}$ is a domain iff n is prime.

20 November 19, 2021

20.1 Prime and maximal ideals

Again, R is commutative.

Remark 20.1 — For F a field, there are two ideals. $F = (1)$ and $(0) \subset F$. This is because all elements of F (besides 0) are units.

Question 20.1 — What if we have a ring whose only 2 ideal are R and (0)?

We claim that R is a field. Any non-zero element generates the whole ring. In other words, $(a) = (1)$, so for any $a \in R$, there is b such that $ab = 1$. Therefore, a is invertible.

Another perspective on this statement is that fields are commutative rings with only 2 ideals.

Prime ideal

Definition (Prime ideal)**.**

1. $P \subsetneq R$ is a **prime ideal** if for all $a, b \in R$ such that $ab \in P$, $a \in P$ or $b \in P$. This is modeled on primes in $\mathbb{Z}$, since if $p \mid ab$, then $p \mid a$ or $p \mid b$.
2. $M \subsetneq R$ is a maximal ideal if there does not exist $y \subseteq R$ such that $M \subsetneq Y \subsetneq R$.

Example 20.1. $\mathbb{Z}$. (p) for p prime is a maximal ideal.

Proposition 20.1.

1. *$P \subsetneq R$ is prime iff R/P is an integral domain.*
2. *$M \subsetneq$ is maximal iff R/M is a field.*

Corollary 20.2.

1. *Maximal ideals are prime (but the reverse implication is not true).*
2. *(0) is prime iff R is an integral domain.*

Proof.

1. Fields are integral domains.
2. $R/(0) = R$.

■

Proposition 20.3. *Any proper ideal in R can be embedded into a maximal ideal.*

Lemma 20.4 (Zorn's lemma)**.** *Let S be a partially ordered set such that any chain has an upper bound. Then S has a maximal element.*

Discussion of partially ordered sets.

1. Partially ordered set in S.
   (a) $x \leq x$.
   (b) $x \leq y$ and $y \leq x$ implies $x = y$.
   (c) Transitivity.
2. Chain (or tower) is a totally ordered subset.
3. Upper bound. For $X \subseteq S$, b is an upper bound if $b \geq x$ for all $x \in X$.
4. $m \in S$ is maximail if $x \geq m$ implies that $x = m$.

Proof. (of the proposition) Let $I \subsetneq R$. Let

$$S = \{\mathcal{J} \subsetneq R \mid I \subset \mathcal{J}\}.$$

We claim that S satisfies the conditions for Zorn's lemma. $\mathcal{J}_1 \leq \mathcal{J}_2 \Leftrightarrow \mathcal{J}_1 \subset \mathcal{J}_2$. Upper bound? Let X be a chain in S.

$$\mathcal{J} = \bigcup_{\mathfrak{A} \in X} \mathfrak{A}$$

is an ideal[3]. $a \in \mathcal{J}$ implies that there exists $\mathfrak{A} \in X$ such that $a \in \mathfrak{A}$. Then $ca \in \mathfrak{A} \subset \mathcal{J}$ for all c. $a, b \in \mathcal{J}$ implies there exists $\mathfrak{A} \in X$ such that $a, b \in \mathfrak{A}$ implies $a + b \in \mathfrak{A}$. By Zorn's, S has a maximal element M, which is a maximal ideal containing I. ■

[3] $\mathfrak{A}$ *is an A.*

> Remark 20.2 — This maximal ideal need not be unique. In $\mathbb{Z}$, $(6) \subseteq (2)$ and $(6) \subseteq (3)$.

Proposition 20.5. *$f : R \to S$ is a ring homomorphism. For $I \subset SS$ an ideal, the pullback of I*

$$f^{-1}(I) = \{a \in R \mid f(a) \in I\}$$

(a pre-image with respect to f),

1. *$f^{-1}(I)$ is an ideal in R, and*
2. *if $q \subset S$ is prime (ideal), then $f^{-1}(q)$ is prime (ideal).*

Remark 20.3 — $I \subset R$ and $R \to^{\pi} R/I$. Correspondence between

$$[I \subset J \subset R] \leftrightarrow [\mathfrak{A} \subset R/I]$$

(prime to prime).

Proposition 20.6. *The intersection of ideals is an ideal.*

20.2 Factoriality

In this section, R will always be commutative integral domains.

Unit

Definition (Unit)**.**

1. $U \in R$ is a unit iff u is invertible.
2. $a \in R$ is irreducible if for any b, c such that $a = bc$, b is a unit or c is a unit.

Remark 20.4 — In $\mathbb{Z}$, primes are irreducible. In $F[x]$, irreducible polynomials are irreducible.

Example 20.2. In $\mathbb{Z}/6\mathbb{Z}$, 1 and 5 are units. 2 and 3 (not?) are irreducible elements. 0 is 0. 4 is none of the above.

Principal ideal domain

Definition (Principal ideal domain)**.** R a commutative integral domain is a **principal ideal domain** (PID) if every ideal is principal.

Example 20.3. $\mathbb{Z}$ is a PID. In fact, prime ideals are maximal ideals.

Remark 20.5 — Field F. There is a ring homomorphism $\varphi : \mathbb{Z} \to F$ that sends $1 \mapsto 1$.

1. φ is injective, in which case $\mathrm{char} F = 0$.
2. $\mathrm{Ker}\varphi \neq (0)$. $\mathbb{Z}/\mathrm{Ker}\varphi \simeq \mathrm{Im}\varphi$ (domain) is a field. Then $\mathrm{Ker}\varphi = (p)$, so $\mathrm{char} F = p$.
3.

21 November 22, 2021

Proposition 21.1. *R is an integral domain.*

1. *Suppose (a) is a prime ideal. Then a is irreducible.*
2. *If R is also a PID, the reverse is true.*

Proof.

1. Assume (a) is prime ($a \neq 0$). Let $a = bc$. Want to show that b or c is a unit. $bc \in (a)$ implies $b \in (a)$ or $c \in (a)$. WLOG, suppose $b \in (a)$. Then $b = ab'$ implies $a = bc = ab'c$. Therefore, $a(1 - b'c)$. We assume $a \neq 0$. Since R is an integral domain, $1 - b'c = 0$, so $b'c = 1$. We conclude that c is a unit.
2. Let $a \in R$ be an irreducible element and suppose (a) is non-prime. Then there exist $b, c \in R$ with $bc \in (a)$ but $b, c \notin (a)$. Consider new ideal (b, a) which strictly contains (a). (b, a) is principal (since R is PID), so it is generated by some element d. $(a) \subset (d) \Rightarrow a \in (d)$, so write $a = da'$. Then since a is irreducible, either a' is a unit or d is a unit. If a' is a unit, then $(a) = (d)$[4]. If d is a unit, we get $(b, a) = (1) = R$, so

   $$1 = aa' + bb' \Rightarrow c = aca' + bcb'.$$

   Then $aca' \in (a)$ and $bcb' \in (a)$ (since $bc \in (a)$), hence (a) is prime.

[4] *If two elements differ by a unit, $a = uc$, then $(a) = (c)$.*

■

R is an (commutative) integral domain.

> **Definition** (Unique factorization domain)**.** R is a **unique factorization domain** or (UFD) if for all $a \in R$, there exists decompostion
>
> $$a = up_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$
>
> where u is a unit, p_i irreducible, $\alpha_i > 0$, which is unique up to reordering, choice of unit, and replacements of p_i by εp_i for unit ε.

Unique factorization domain

We may say that a ring is "factorial" which is equivalent to saying that is a UFD.

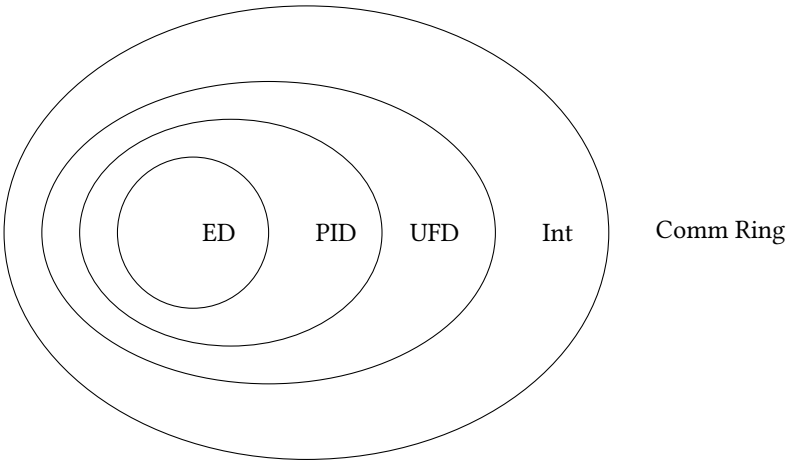
Theorem 21.2. *PID is a UFD.*

Proof. There exists

$$S = \{(a) \mid a \text{ does not have factorization}\}$$

a set of ideals in R. Want to show that $S = \varnothing$. Assume S is non-empty. Suppose we have a chain (a_i) in S. Let $(b) = \cup(a_i)$ (ideals are principal in PID). But then $b \in (a_i)$ for some i, so $(b) \subset (a_i)$. By definition $(a_i) \subset (b)$. Then $(a_i) = (b) \Rightarrow (b) \in S$. Therefore we can use Zorn's. There exists maximal element $(d) \in S$. d is not irreducible (otherwise $d = d$ is a trivial factorization). Then $d = d_1 d_2$, not units, and

$(d) \subsetneq (d_1), (d_2)$. This implies $(d_1), (d_2) \notin S$, since (d) was maximal element. Hence d_1, d_2 have factorizations, which implies d has factorization. Uniqueness an exercise (exactly as for $\mathbb{Z}$ using (a) prime equivalent to a irreducible). ■



Inclusion structure of our objects. All are proper.

Example 21.1.

1. The Gaussian integers
$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$
are a Euclidean domain.
2. Let $\omega^3 = 1$, and consider
$$\mathbb{Z}[\omega] = \{a + b\omega + c\omega : a, b, c\, in \mathbb{Z}\},$$
also a Euclidean domain.
3. Consider
$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5}\}.$$
Notice that $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. One can show that these are irreducible, so this is not a UFD.

Field of fractions (special case of "localizations"). Start with integral domain R. Define equivalence relation on $\mathbb{R} \times \mathbb{R}^\times$ where $(a, b) \sim (c, d)$ if $ad = bc$. Then $F = \text{Frac}(R)$ to be the set of equivalence classes (a, b), denoted $\frac{a}{b}$. Claim: F is a field.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bc}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Example 21.2. $F \to \mathbb{Q}$, $F[x] \to F(x)$

22 November 24, 2021

22.1 Midterm Solutions

Problem 2. $G = \{f : \mathbb{R}^2 \to \mathbb{R}^2, f = Ax + b\}$. $T = \{x + b\}$ and $R = \{Ax\}$, with $b \in \mathbb{R}^2$ and $AA^T = I$. Check that

1. T is normal,
2. $T \cap R = \{I\}$, and
3. $TR = G$.

Checking.

1. For $t \in T$ given by $t(x) = x + b$ and $\rho \in R$ given by $\rho(x) = Ax$,
$$\rho \circ t \circ \rho^{-1}(x) = A(A^T x + b) = x + Ab$$
2. R, T act on the plane. All elements of R fix the origin. No elements of T do this besides the identity. Therefore their intersection is only the identity.
3. $f = Ax + b = (Ax) + b = A(x + A^T b)$, so R, T generate everything.

Problem 3. G nilpotent. $(e < G_n \triangleleft G_{n-1} \triangleleft \ldots \triangleleft G_1 \triangleleft G)$. $N \triangleleft G$. Show that there is a central series passing through N.

Lemma 22.1. *Any refinement of a central series is central.*

Proof. We'll use $[G_i, G] < G_{i+1}$.

$$e < G_n \triangleleft \ldots \triangleleft G_{i+1} < \Gamma < G_i \triangleleft \ldots \triangleleft G_1 \triangleleft G$$

Observe t hat

$$[\Gamma, G] < [G_i, G] < G_{i+1}$$
$$[G_i, G] < G_{i+1} < \Gamma$$

■

By Shreier's theorem, our given series and the series $\{e\} \triangleleft N \triangleleft G$ have a common refinement. This common refinement is what we want.

Problem 4.

1. 3-Sylow subgroup of A_6 has order 9. There are two possible groups of order 9. A_6 has no element of order 9. Alternatively, exhibit $\langle (1\ 2\ 3), (4\ 5\ 6) \rangle$.
2. How many? $|A_6| = 360$. $N_3 \equiv 1(\pmod 3)$. $N_3 \mid 40$. Our choices for N_3 are 1, 4, 10, and 40. There is a one-to-one correspondence between 3-Sylow subgroups and ways to split $[6]$ in half, since all 3-Sylow subgroups are $Z_3 \times Z_3$. Then $N_3 = \frac{1}{2}\binom{6}{3} = 10$.

3. Next possible think to check is S_9, so the 3-Sylow subgroup has order 81. Claim that the 3-Sylow subgroup of S_9 is not abelian. We don't have 4 disjoint 3-cycles, so $(Z_3)^4$ is not possible. Argue similarly for $(Z_9)^2, Z_{81}, Z_0 \times (Z_3)^2$. Alternatively, consider

$$\langle (1\ 2\ 3), (4\ 5\ 6), (7\ 8\ 9), (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9) \rangle.$$

This is

$$(Z_3 \times Z_3 \times Z_3) \rtimes Z_3$$

and can be written as the wreath product

$$Z_3 \wr Z_3.$$

This generalizes to $G, H < S_n$, with $G \wr H = G^n \rtimes H$.

Problem 5. p the minimal prime that divides the order of G. Want to show if H has index p, then $H \triangleleft G$.

Choose $X = G/H$. G acts on X by left multiplication. $G \to^{\rho} S(X)$.

Lemma 22.2. *Kerρ (the core of H) is the maximal normal subgroup of H.*

$$\text{Ker}\rho = \bigcap_{x \in G} xHx^{-1}$$

Ker$\rho < H$. Indeed, $g \in$ Ker$\rho \Rightarrow gH = H$, so $g \in H$.

For us, $\rho : G \to S(X) = S_p$. Im$\rho < S_p$ and $G/\text{Ker}\rho \simeq \text{Im}\rho$. Recall that $|X| = p$. Then $|\rho|$ divides $p!$ and $|G|$. Since p is the smallest prime that divides $|G|$, we must have the image of ρ has size 1 or p. The right choice is p, since 1 would imply the kernel is the entire group (which is false because H is a strict subgroup). $|G : \text{Ker}\rho| = p$ and $|G : H| = p$. Ker$\rho < H$, so Ker$\rho = H$. Therefore $H \triangleleft G$.

23 December 1, 2021

23.1 Field extensions

Proposition 23.1. *Say F is a field. Then $F[x]$ is a PID.*

Proof. $F[x]$ is a ED (hw) which are all PIDs. ■

Extension

Definition (Extension)**.** Suppose we have fields $F \subset L$. Then L is an **extension** of F.

Remark 23.1 — L/F a field extension gives us that L is an F vector space.

degree

Definition (degree)**.** The **degree** of an extension is $[L : F] = \dim_F L$. L/F is finite if its degree is finite and infinite otherwise.

Example 23.1.

1. $\mathbb{C}/\mathbb{R}$. $[\mathbb{C} : \mathbb{R}] = 2$, and we can write $\mathbb{C} = \mathbb{R} + \mathbb{R}i$.
2. Fraction field

$$\text{Frac}(\mathbb{R}[x]) = \mathbb{R}(x) = \{f(x)/g(x) : f, g \in \mathbb{R}[x], g \neq 0\}$$

   $\mathbb{R}(x)/\mathbb{R}$ is infinite (transcendental).
3. Consider $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$. This has degree 2.

Proposition 23.2. *For a tower of extensions, $L/K/F$, the degree can be computed transitively.*

$$[L : F] = [L : K][K : F]$$

Algebraic

Definition (Algebraic)**.** Suppose we have L/F and $\alpha \in L$

1. we say that α is **algebraic** over F if there exists polynomial $0 \neq f(x) \in F[x]$ such that $f(\alpha) = 0$.
2. L/F is algebraic if every element of L is algebraic.
3. L/F is **transcendental** if it is not algebraic.

Example 23.2. Consider $i \in \mathbb{C}$ viewing the extension $\mathbb{C}/\mathbb{R}$. i satisfies $x^4 - 1$, i.e. it is a fourth root of unity. The *right* equation to think about, however, is $x^2 + 1 = 0$.

Given $\alpha \in L \setminus F$ in extension L/F, there is a unique ring homomorphism $F[x] \to^{\varphi_\alpha} L$ such that $x \mapsto \alpha$ and F is sent to itself. We claim that Ker $\varphi_\alpha \neq 0$ iff α is algebraic. Indeed, $p(x) \in$ Ker φ_α iff $\varphi_\alpha(p(x)) = p(\alpha) = 0$. Ker φ_α is an ideal in $F[x]$ (a PID), so Ker $\varphi_\alpha = (p(x))$ for some $p(x) \in F[x]$. Note that (first isomorphism theorem)

$$F[x]/(p(x)) \simeq \text{Im } \varphi_\alpha.$$

Im φ_α is a domain, so $(p(x))$ is prime. Then we conclude that $p(x)$ is irreducible.

Minimal polynomial

Definition (Minimal polynomial)**.** The **minimal polynomial** of α, denoted $\text{Irr}_F(\alpha)$ to be the monic generator of the ideal Ker φ_α, i.e.

$$\text{Ker } \varphi_\alpha = (\text{Irr}_F(\alpha)) .$$

Remark 23.2 — $\alpha \in L/F$ algebraic over F. $p(x) = \text{Irr}_F(\alpha)$ is a maximal ideal, so

$$F[x]/(p(x)) \simeq \text{Im } \varphi_\alpha \subset L$$

is a field. This we can denote as $F[\alpha] = F(\alpha)$.

24 December 3, 2021

Reminder from last time: $\alpha \in L/F$. $F[x] \to^{\varphi_\alpha} L$ with $f \mapsto f(\alpha)$. Ker $\varphi_\alpha = (p(x))$ prime implies it is maximal. $F[x]$ is a PID. Take $p(x)$ monic. Then $\operatorname{Irr}_F(\alpha) = p(x)$.

Minimal subfield

Definition (Minimal subfield)**.** For L/F and $\alpha \in L$, $F(\alpha)$ is the **minimal subfield** of L containing α.

Remark 24.1 — $F(\alpha)$ is the intersection of all fields $K \subset L$ where $\alpha \in K$.

Proposition 24.1. *L/F, $\alpha \in L$ is algebraic. Then*

1. *$F[\alpha] = \left\{\sum a_i \alpha^i : a_i \in F, n \geq 0\right\}$ is a field (and $F[\alpha] = F(\alpha)$),*
2. *$F(\alpha)/F$ is finite, and*
3. *$[F(\alpha) : F] = \deg \mathit{Irr}_F(\alpha)$.*

Proof.

1. We have $F[x] \to^{\varphi_\alpha} L$ where $f \mapsto f(\alpha)$. Then Im $\varphi_\alpha = F[\alpha]$. By the first isomorphism theorem,

$$\text{Im } \varphi_\alpha \simeq \frac{F[x]}{\text{Ker } \varphi_\alpha} = \frac{F[x]}{(p(x))}.$$

   $(p(x))$ is prime since Im $\varphi_\alpha \subset L$ is a domain. Since $F[x]$ is a PID, prime implies maximal. Hence, $(p(x))$ maximal implies Im φ_α is a field. (Note: We proved that any $f(\alpha) = \sum a_i \alpha^i$ has an inverse in $F[\alpha]$.) $F(\alpha) = F[\alpha]$. Clearly $F[\alpha] \subset F(\alpha)$, but $F[\alpha]$ is already a field. For explicitness, we write

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in F[x], g(x) \neq 0 \right\}$$

2. Indeed, $F(\alpha) = F[\alpha]$ is generated by $\{1, \alpha, \ldots, \alpha^{n-1}$ where $n = \deg p(x)$, so $\dim_F F(\alpha) \leq n$.
3. WTS $\dim_F F(\alpha) = n$, since by definition, $[F(\alpha) : F] = \dim_F F(\alpha)$. Why can't it be smaller? BWOC suppose $\dim_F F(\alpha) = m < n$. Then $\{1, \alpha, \ldots, \alpha^m\}$ is linearly dependent, so there exists $g(x) \in F[x]$ with degree m such that $g(\alpha) = 0$. But then $g(x) \in$ Ker φ_α which implies $g(x) \in (p(x))$. Then $p(x) \mid g(x)$. In other words,

$$n = \deg p(x) \leq \deg g(x) = m.$$

   Contradiction.

■

Corollary 24.2. *$\alpha \in L/F$ is algebraic iff $F(\alpha)/F$ is finite.*

Question 24.1 — Can we have an algebraic extension L/F not finite? Yes. We can take the following examples.

$$\mathbb{Q}\left(\left\{\sqrt{n} : n \in \mathbb{Z}\right\}\right), \quad \mathbb{Q}\left(\left\{\sqrt[n]{2} \mid n \in \mathbb{Z}\right\}\right)$$

So algebraic does not imply finite. The other direction, however, is true. Any finite extension is algebraic.

Definition. $\alpha_1, \ldots, \alpha_n \in L/F$. $F(\alpha_1, \ldots, \alpha_n)$ is the minimal field containing $\alpha_1, \ldots, \alpha_n$. We can also define it as a composition of extensions.

$$F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1)(\alpha_2)\ldots(\alpha_n)$$

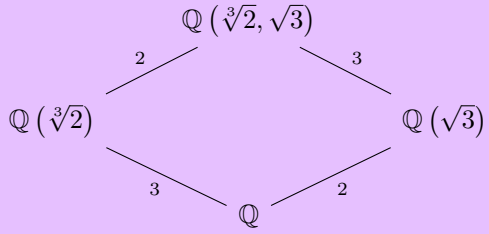
Corollary 24.3. *If we take $\alpha_1, \ldots, \alpha_n \in L/F$ all algebraic, then $F(\alpha_1, \ldots, \alpha_n)$ is finite (and hence algebraic).*

Proof. Induction, using proposition. ■

Example 24.1. Consider the extension $\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right)/\mathbb{Q}$. We can compute

$$[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right) : \mathbb{Q}] = 6$$

by considering the extension as a tower and noticing the degree splits nicely.



We get for example that $\sqrt[3]{2} + \sqrt{3}$ is algebraic. Moreover, there exists $g(x) \in F[x]$ such that $g\left(\sqrt[3]{2} + \sqrt{3}\right) = 0$, whose degree is 6.

Example 24.2.

1. $\mathbb{C} = \mathbb{R}(i)$ with degree $[\mathbb{C} : \mathbb{R}] = 2$ is in a sense, the most interesting field extension of degree 2.
2. $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ (minimal polynomial $x^2 - 2$) has degree $[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}] = 2$.

Proposition 24.4. *The property of being algebraic (for field extensions) is transitive. For $E/L/F$, if L/F is algebraic and E/L is algebraic, then E/F is algebraic.*

Proof. WTS that for any $\alpha \in E$, $F(\alpha)/F$ is finite. We know that α is algebraic over L. Hence, there exists $\beta_0, \beta_1, \ldots, \beta_n \in L$ such that for $f(x) = \sum \beta_i x^i$, $f(\alpha) = 0$. Since L/F is algebraic, $F(\beta_0, \ldots, \beta_n)/F$ is finite. Then

$$F(\alpha, \beta_0, \ldots, \beta_n)/F$$

is finite.

$$F(\alpha) \subset F(\alpha, \beta_0, \ldots, \beta_n)$$

The RHS is finite, so the LHS must be finite. ■

24.1 Field automorphisms and the algebraic closure

We will construct $F^{\text{alg}} \supset F$ such that any α algebraic in $F^{\text{alg}}(\alpha)$ is already in F^{alg}. One such example is $\mathbb{C}/\mathbb{R}$. Such field extensions are called algebraically closed.

25 December 6, 2021

Observation: $\sigma : L \to K$ a ring homomorphism between fields, must be injective. This is because Kerσ is an ideal. Since the kernel is not the whole field, it must just be the zero ideal (recall that fields have exactly two ideals).

For L/F we write

$$\begin{aligned}\mathrm{Aut}_F(L) = \{\sigma : L \to L \mid \sigma_F = \mathrm{id}_F \\ L \xrightarrow{\sigma} L \\ \cup \qquad\quad \cup \\ F \xrightarrow{=} F\end{aligned}$$

Lemma 25.1. *L/F algebraic. $\sigma : L \to L$ field homomorphism with $\sigma_F = id$. Then $\sigma \in Aut_F(L)$ (σ is an isomorphism).*

Proof. Only need to show σ is surjective. Want to show it is in the image of σ. Let $f(x) \in F[x]$ such that $f(\alpha) = 0$. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be all the roots of f in L. Claim: $\sigma(\alpha_i) = \alpha_j$, i.e. σ takes roots to roots. Indeed, if $f(x) = \sum a_i x^i$,

$$\sigma(f)(x) = \sum \sigma(a_i) x^i = f(x).$$

For β root of f, then

$$f(\sigma(\beta)) = \sum a_i (\sigma(\beta_i))^i = \sum a_i \sigma(\beta^i) = \sum \sigma(a_i)\sigma(\beta^i) = \sigma\left(\sum a_i \beta^i\right) = \sigma(f(\beta)) = 0.$$

Therefore, σ must permute the roots α_i (remember σ is injective). Thus, there exists j such that $\sigma(\alpha_j) = \alpha_1 = \alpha$. ∎

Goal: for all f, there exists F^{alg}/F.

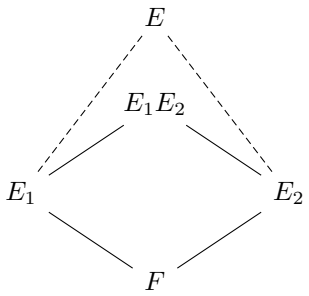
Proposition 25.2. *For all $f(x) \in F[x]$ of degree at least 1, there exists l/F such that f has a root in L.*

Proof. Assume $f(x)$ is irreducible. Let $\tilde{L} = F[x]/(f(x))$. $f(x)$ is irreducible implies that $(f(x))$ is prime (note that $F[x]$ is PID), which in turn implies $(f(x))$ is maximal, so $\tilde{L}$ is a field. What are the elements? They are $\overline{g(x)} = g(x) \mathrm{mod} f(x)$.

$$F \to^{\sigma} \tilde{L} = \frac{F[x]}{(f(x))} \quad a \mapsto \overline{a} = a \mathrm{mod} f(x)$$

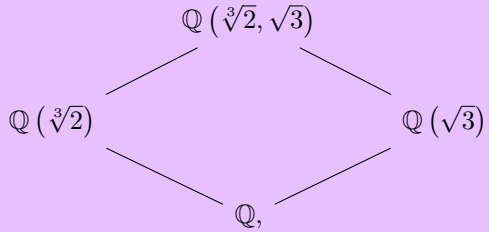
Let $X = \tilde{L} \backslash \sigma(F)$ and $L = S \coprod F$ with field operations defined in an obvious way. ∎

Terminology

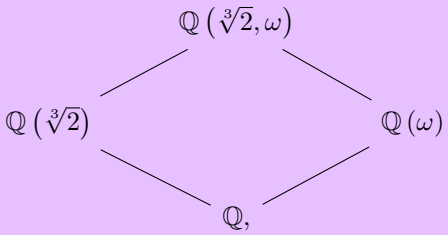


E_1E_2 field composite is the minimal extension containing E_1, E_2.

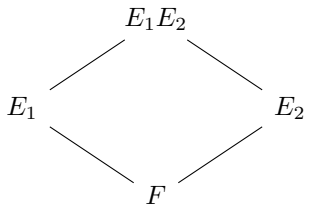
Example 25.1.



Example 25.2. Let $\omega = e^{2\pi i/3}$, which has minimal polynomial $x^2+x+1 = 0$.



Lemma 25.3. *$\sigma : E \to L$ a field homomorphism, then $\sigma(E_1E_2) = \sigma(E_1)\sigma(E_2)$.*



Definition. E is **algebraically closed** if every $f(x) \in E[x]$ of degree at least 1 has a root in E.

Theorem 25.4. *For all F, there exists $\overline{F}/F$ such that $\overline{F}$ is algebraically closed.*

Proof. 1. We'll construct an extension L/F such that any $f(x) \in F[x]$ with degree at least 1 has a root in L.

$$\{f\}_{f\in F[x]} \to \{X_f\}_{f\in F[x]}$$

Let $A = F[X_f \mid f \in F[x]]$. Consider the ideal $I = \langle f(X_f)\rangle_{f\in F[x]}$ in A.

$$f = \sum a_i x^i \in F[x], \quad \sum a_i X_f^i \in A$$

We want to consider A/I. Want to show that $I \neq (1)$ (that is, I is proper).

■

26 December 10, 2021

Example 26.1. Let $F = \mathbb{F}_2$. Then

$$A = \mathbb{F}_2[X_f]_{f \in \mathbb{F}_2[x]}$$

where

$$\mathbb{F}_2[x] = \{a_0 + a_1 x + \ldots + a_n x^n\}.$$

These can be viewed as binary sequences, and each X_f is a variable corresponding to a binary number.

$$A = \lim_{n \to \infty} \mathbb{F}_2[X_{\{0,1\}^n}], \quad I = \langle f(X_f) \rangle$$

$$f_0 = 1, \quad f_1 = 1, \quad f_{01} = x, \quad f_{11} = x + 1, \quad f_{101} = x^2 + 1$$

each with their corresponding $X_0, X_1, \ldots$.

Theorem 26.1. *For all F, there exists L ($F \subset L$) such that L is algebraically closed.*

Proof. Recall that we let

$$A = F[X_f]_{f \in F[x]} \quad \text{and} \quad \langle f(X_f) \rangle_{f \in F[x], f \neq c}$$

We claim that $I \neq (1)$. Suppose $I = (1)$. Then there exists some set of $f_i(X_{f_i}) \in I$ and $g_i \in A$ such that

$$\varphi = \sum g_i f_i(X_{f_i}) = 1.$$

We can write

$$g_i = g_i \left(X_{f_{i_1}}, X_{f_{i_2}}, \ldots, X_{f_{i_{n_i}}} \right)$$

Recall that for all $f \in F[x]$, there exists $/F$ where f has a root. Hence, there exists E/F such that $f_1, \ldots, f_n$ all have roots in E (inductively, say). Consider

$$A \subset B = E[X_f]_{f \in F[x]}.$$

φ is certainly in B. Let α_i be a root of $f_i \in E$. Plugin $X_{f_i} = \alpha_i \in \varphi$ to get

$$\sum g_i(\ldots) f_i(\alpha_i) = 0,$$

but $\varphi = 1$. This proves our claim that $I \neq (1)$, i.e. $I \subsetneq A$. Let $I \subset \mathcal{M} \subset A$, $\tilde{L}_1 = A/\mathcal{M}$, $F \to \tilde{L}_1$, injective map (identification). Any $f \in F[x]$ has a root in $\tilde{L}_1$, where this root is precisely $\overline{X}_f = X_f \bmod \mathcal{M}$. Now iterate. $F \to \tilde{L}_1 \to \tilde{L}_2 \to \ldots$. Let L be the union of all $\tilde{L}_i$. We claim that L is algebraically closed. Indeed, $\varphi[x] \in L[x]$. Then $\varphi[x] \in \tilde{L}_n[x]$ implies that it has roots in $\tilde{L}_{n+1}$. ∎

Note that saying any polynomial has a root in a field leads to the same thing as saying any polynomial has all roots in a field, since just divide by $x - \alpha$, giving a new polynomial, and repeat.

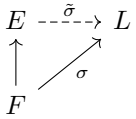
> **Definition.** $F^{\text{alg}} = \overline{F}$ is a minimal algebraically closed field containing F.

We claim that this exists (just take intersection of all).

Example 26.2. $\mathbb{R} \subset \mathbb{C}$, as we know and love. $\mathbb{Q} \subset \mathbb{Q}^{\text{alg}}$ is not all of $\mathbb{C}$.

Proposition 26.2. *Extension of homomorphisms.*

1. *L algebraically closed. $F \to^{\sigma} L$ a field monomorphism. Let E/F be an algebraic extension. Then there exists a unique map $\tilde{\sigma} : E \to L$ such that*



   the diagram commutes.

2. *Any 2 algebraic closures F are isomorphic.*

Note that since $\tilde{\sigma}$ is not unique, the isomorphism is not canonical.