Groups, Rings, and Modules

Jonathan Gai

February 8, 2022

Contents

Lecture 1: Groups

20 Jan. 12:00

Introduction

Groups

Continuation from IA, focussing on

1. Simple groups, p-groups, p-subgroups.
2. Main results in this part of the course will be the Sylow Theorems.

Rings

Sets where you can add, subtract and multiply.

Example. Examples of rings include,

1. $\mathbb{Z}$ or $\mathbb{C}[X]$.
2. Rings of integers $\mathbb{Z}[i], \mathbb{Z}[\sqrt{2}]$ (More in Part II Number Fields).
3. Polynomial rings $\mathbb{C}[x_1, \ldots, x_2]$ (More in Part II Algebraic Geometry).

A ring where you can divide is called a *field.*

Example. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{Z}/p\mathbb{Z}$ for p prime.

Modules

An analogue of vector space where the scalars belong to a ring instead of a field.

We will classify modules over certain nice rings.

Allows us to prove Jordan normal form, and classify finite Abelian groups.

1 Groups

1.1 Revision and Basic Theory

We revisit basic properties and definition from Part IA Groups.

Definition 1.1 (Group). A *group* is a pair $(G, \cdot)$ where G is a set and $\cdot : G \times G \to G$ is a binary operation satisfying:

1. (Associativity) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2. (Identity) $\exists a \in G$ s.t. $e \cdot g = g \cdot e = g \ \forall g \in G$.
3. (Inverses) $\forall g \in G, \exists y^{-1} \in G$ s.t. $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Remark. Some things to note form definition of a group.

1. *Closure* is included implicitly in the definition of a binary operation. In checking $\cdot$ well-defined, we need to check closure, i.e. $a, b \in G \implies a \cdot b \in G$.
2. If using additive (or multiplicative) notation, often write 0 (or 1) for identity.

Definition 1.2 (Subgroup). A subset $H \subset G$ is a *subgroup* (written $H \leq G$) if $h \cdot h^{-1} \in H, \forall h, h' \in H$, and $(H, \cdot)$ is a group. Remark: A non-empty subset H of G is a subgroup if $a, b \in H \implies a \cdot b^{-1} \in H$

Example. Here we list some common groups and their subgroups.

1. Additive $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.
2. Cyclic and dihedral group, $C_n \leq D_{2n}$.
3. Abelian groups - those $(G, \cdot)$ such that $a \cdot b = b \cdot a \ \forall a, b \in G$
4. Symmetric and Alternating groups, $A_n \leq S_n$.
5. Quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.
6. General and Special Linear Groups, $SL_n(\mathbb{R}) \leq SL_n(\mathbb{R})$.

Definition 1.3 (Direct Product). The *(direct) product* of groups G and H is the set $G \times H$ with operation given by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2).$$

Let $H \leq G$, the *left cosets* of H in G are the sets $gH = \{gh \mid h \in H\}$ for $g \in G$. These partition G, and each coset has the same cardinality as H. So we can deduce.

Theorem 1.1 (Lagrange's Theorem). Let G be a finite group and $H \leq G$, Then $|G| = |H| \cdot [G : H]$ where $[G : H]$ is the number of left cosets of H in G. $[G : H]$ is the *index* of H in G.

Remark. Can also carry this out with right cosets. Lagrange's Theorem then implies that the number of left cosets is the same as the number of right cosets.

Definition 1.4 (Order). Let $g \in G$. If $\exists n \geq 1$ s.t. $g^n = 1$ then the least such n is the *order* of g, otherwise we say that g has infinite order.

Remark. If g has order d, then

1. $g^n = 1 \implies d \mid n$.
2. $\{1, g, \ldots, g^{d-1}\} \leq G$ and so if G is finite, then $d \mid |G|$ (by Lagrange's Theorem).

Definition 1.5 (Normal Subgroup). A subgroup $H \leq G$ is *normal* if $g^{-1}Hg = H$ $\forall g \in G$. We write $H \trianglelefteq G$.

Proposition 1.1. If $H \trianglelefteq G$ then the set G/H of left cosets of H in G is a group (called the *quotient group*) with operation

$$g_1H \cdot g_2H = g_1g_2H.$$

Proof. Check that $\cdot$ is well-defined.

Suppose $g_1H = g_1'H$ and $g_2H = g_2'$. Then $g_1' = g_1h_1$ and $g_2' = g_2h_2$ for some $h_1, h_2 \in H$, we have

$$\begin{aligned} g_1'g_2' &= g_2h_1g_2h_2 \\ &= g_1g_2(g_2^{-1}h_2g_2)h_2 \end{aligned}$$

so $g_1'g_2'H = g_1g_2H$.

Associativity is inherited from G, the identity is $H = eH$, and the inverse of gH is $g^{-1}H$. ■

Definition 1.6 (Homomorphism). G, H groups. A function $\phi : G \to H$ is a group homomorphism if $\phi(g_1g_2) = \phi(g_1)\phi(g_2) \forall g_1, g_2 \in G$. It has *kernel*

$$\ker(\phi) = \{y \in G \mid \phi(y) = 1\} \trianglelefteq G,$$

and *image* $\mathrm{Im}(\phi) = \{\phi(y) \mid y \in G\} \leq H$.

Proof. If $a \in \ker(\phi)$ and $g \in G$, then

$$\begin{aligned} \phi(g^{-1}ag) &= \phi(g^{-1})\phi(a)\phi(g) \\ &= \phi(g^{-1})\phi(g) \\ &= \phi(g^{-1}g) \\ &= \phi(1) \\ &= 1. \end{aligned}$$

So it is indeed a normal subgroup. ■

Lecture 2: Isomorphism Theorems

22 Jan. 12:00

We will next talk about a special kind of homomorphism.

Definition 1.7. An *isomorphism* of groups is a group homomorphism that is also a bijection.

We say that G and H are isomorphic (written $G \cong H$) if there exists an isomorphism $\phi : G \to H$.

Exercise. Check that $\phi^{-1} : H \to G$ is a group homomorphism.

Theorem 1.2 (First Isomorphism Theorem). Let $\phi : G \to H$ be a group homomorphism. Then $\ker(\phi) \trianglelefteq$ and $G/\ker(\phi) \cong \operatorname{Im}(\phi)$.

Proof. Let $K = \ker(\phi)$. We already checked that K is normal.

Define $\Phi : G/K \to \operatorname{Im}(\phi)$, $gK \mapsto \phi(g)$. We need to check that Φ is well-defined first.

$$\begin{aligned} g_1K = g_2K &\iff g_2^{-1}g_1 \in K \\ &\iff \phi(g_2^{-1}g_1) = 1 \\ &\iff \phi(g_1) = \phi(g_2). \end{aligned}$$

Note that we showed that Φ is injective at the same time because we can just go the other way.

Next, we show that Φ is a group homomorphism.

$$\begin{aligned} \Phi(g_1Kg_2K) &= \Phi(g_1g_2K) \\ &= \phi(g_1g_2) \\ &= \Phi(g_1K)\Phi(g_2K). \end{aligned}$$

Lastly, we show that Φ is surjective. Let $x \in \operatorname{Im}(\phi)$, say $x = \phi(g)$ for some $g \in G$, then $x = \Phi(gK)$. So it is indeed an isomorphism. ■

Example. If we consider the function

$$\begin{aligned} \phi \colon \mathbb{C} &\longrightarrow \mathbb{C}^\times \\ z &\longmapsto e^z \end{aligned}$$

Since $e^{z+w} = e^z e^w$, this is a group homomorphism from $(\mathbb{C}, +) \to (\mathbb{C}, \times)$. It is well known that

$$\begin{aligned} \ker(\phi) &= 2\pi i\mathbb{Z}, \\ \operatorname{Im}(\phi) &= \mathbb{C}^\times \quad \text{by existence of log }. \end{aligned}$$

Thus, $\mathbb{C}/2\pi i\mathbb{Z} \cong \mathbb{C}^\times$.

From the naming for the First Isomorphism Theorem, we have the following Isomorphism Theorems as well.

Theorem 1.3 (Second Isomorphsim Theorem). Let $H \leq G$, and $K \trianglelefteq G$. Then $HK = \{hk \mid h \in H, k \in K\} \leq G$ and $H \cap K \trianglelefteq H$. Moreover,

$$\frac{HK}{K} \cong \frac{H}{H \cap K}.$$

Proof. Let $h_1k_1, h_2k_2 \in HK$ with $h_1, h_2 \in H$, $g_1, g_2 \in G$. It suffices to show that

$$h_1k_1(h_2k_2)^{-1} = \underbrace{h_1h_2^{-1}}_{H}\underbrace{(h_2k_1k_2^{-1}h_2^{-1})}_{K} \in HK.$$

Thus, $HK \leq G$ by remark from last lecture. Let

$$\begin{aligned} \phi \colon H &\longrightarrow G/K \\ h &\longmapsto hK. \end{aligned}$$

This is the composition of inclusion map $H \to G$ and quotient map $G \to G/K$ hence ϕ is a group homomorphism.

$$\begin{aligned} \ker(\phi) &= \{h \in H \mid hK = K\} = H \cap K \trianglelefteq H, \\ \operatorname{Im}(\phi) &= \{hK \mid h \in H\} = HK/K. \end{aligned}$$

First isomorphism theorem gives

$$\frac{HK}{K} \cong \frac{H}{H \cap K}.$$

■

Remark. Suppose $K \trianglelefteq G$, there is a bijection

$$\begin{aligned} \{\text{Subgroups of } G/K\} &\longleftrightarrow \{\text{Subgroups of } G \text{ containing } K\}, \\ x &\longmapsto \{g \in G \mid gK \in X\}, \\ H/K &\longleftarrow H. \end{aligned}$$

Restricts to a bijection between the normal subgroups.

$$\{\text{Normal subgroups of } G/K\} \longleftrightarrow \{\text{Normal subgroups of } G \text{ containing } K\}.$$

Theorem 1.4 (Third Isomorphism Theorem). Let $K \leq H \leq G$ be normal subgroups of G. Then

$$\frac{G/K}{H/K} \cong \frac{G}{H}.$$

Proof. Let

$$\begin{aligned} \phi \colon G/K &\longrightarrow G/H \\ gK &\longmapsto gH. \end{aligned}$$

If $g_1 K = g_2 K$, then $g_2^{-1} g_1 \in K \leq H \implies g_1 H = g_2 H$. So ϕ is well-defined.

ϕ is a surjective group homomorphism with $\ker(\phi) = H/K$.

Now apply First Isomorphism Theorem. ■

If $K \trianglelefteq G$, then studying the group K and G/K gives some information about G.

This approach is not always available.

Definition 1.8 (Simple Group). A group G is *simple* if $\mathbf{1}$ (the trivial subgroup) and G are its only normal subgroups.

Notation. We do not consider the trivial group to be a simple group.

Similar to the prime numbers, we can think of finite simple groups as the building block of finite groups. One of the greatest achievements in math is that we classified *all* finite simple groups!

Lemma 1.1. Let G be an Abelian group. G is simple if and only if $G \cong C_p$ for some prime p.

Proof. We prove the $\impliedby$ direction first. Let $H \leq C_p$. Lagrange's Theorem tells us

$$|H| \big| |C_p| = p.$$

So $|H| = 1$ or p by primality of p. That is, $H = \{1\}$ or C_p. Thus, C_p is simple.

To prove the $\implies$ direction. Let $1 \neq g \in G$. G contains the subgroup

$$\langle g \rangle = \langle \ldots, g^{-2}, g^{-1}, e, g, g, \ldots \rangle$$

which is the subgroup generated by g. It is normal in G since G is Abelian. Since G simple, $\langle g \rangle = G$.

If G is infinite, $G \cong (\mathbb{Z}, +)$ which cannot be true by simplicity of G because $2\mathbb{Z} \trianglelefteq \mathbb{Z}$.

Otherwise, $G \cong C_n$ for some n, let g be a generator. If $m \mid n$, then $g^{n/m}$ generates a subgroup of order m. Because G is simple, the order of the subgroup can only be 1 or n. So the only factors of n is 1 and n, and we have n prime. ■

Lemma 1.2. If G is a finite group, then it has a composition series

$$\mathbf{1} \cong G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_m \cong G$$

with each quotient ${}^{G_{i+1}}/_{G_i}$ simple.

Note that G_i need not be normal in G.

Lecture 3

25 Jan. 1:00

Proof. Induct on $|G|$. When $|G| = 1$, the statement is obviously true.

If $|G| > 1$, let G_{m-1} be a normal subgroup of the largest possible order that is not $|G|$. By the correspondence theorem, ${}^{G}/_{G_{m-1}}$ is simple.

Apply inductively to G_{m-1}. ■

1.2 Group Action

Definition 1.9. For X a set, let $\mathrm{Sym}(X)$ be the group of all bijections $X \to X$ under composition. The identity is $id = id_X$.

A group G is a *permutation group* of degree n if $G \leq \mathrm{X}$ with $|Z| = n$.

Example.

1. $S_n = \mathrm{Sym}(\{1, 2, \ldots, n\})$ is a permutation group of degree n, as is $A_n \leq S_n$.
2. D_{2n}, the symmetries of regular n-gon, is a subgroup of $\mathrm{Sym}(n)$.

Definition 1.10. An *action* of a group G on a set X is a function $* : G \times X \to X$ satisfying

1. $e * x = x$ for all $x \in X$,
2. $(g_1 g_2) * x = g_1 * (g_2 * x)$ for all $g_1, g_2 \in G, x \in X$.

Proposition 1.2. An action of a group G on a set X is equivalent to specifying a group homomorphism $\phi : G \to \mathrm{Sym}(X)$.

Proof. For each $g \in G$ let $\phi_g : X \to X$, $x \mapsto g * x$. We have

$$\begin{aligned}
\phi_{g_1 g_2}(x) &= (g_1 g_2) * x \\
&= g_1 * (g_2 * x) \\
&= \phi_{g_1}(g_2 * x) \\
&= \phi_{g_1} \circ \phi_{g_2}(x).
\end{aligned}$$

Thus, $\phi_{g_1 g_2} = \phi_{g_1} \phi_{g_2}$.

In particular $\phi_{g_1} \circ \phi_{g_1^{-1}} = \phi_{g_1^{-1}} \circ \phi_{g_1} = \phi_e = id_X$.

Because ϕ_g has an inverse, it is bijective. So $\phi_g \in \mathrm{Sym}(X)$. Define

$$\begin{aligned} \phi \colon G &\longrightarrow \mathrm{Sym}(X) \\ g &\longmapsto \phi_g \end{aligned}$$

which is indeed a group homomorphism.

Conversely, let $\phi : G \to \mathrm{Sym}(X)$ be a gruop homomorphism.

Define

$$\begin{aligned} * \colon G \times X &\longrightarrow X \\ (g, x) &\longmapsto \phi(g)(x). \end{aligned}$$

Then it does satisfy the requirements for a group action,

1. $e * x = \phi(e)(x) = id_X(x) = x$,
2. $\begin{aligned}[t] (g_1 g_2) * x &= \phi(g_1 g_2)(x) \\ &= \phi(g_1)(\phi(g_2)(x)) \\ &= g_1 * (g_2 * x). \end{aligned}$

■

Definition 1.11. We say $\phi : G \to \mathrm{Sym}(X)$ is a *permutation representation* of G.

Definition 1.12. Let G act on a set X.

1. The *orbit* of $x \in X$ is $\mathrm{orb}_G(x) = \{g * x \mid g \in G\} \subseteq X$
2. the *stabilizer* of $x \in X$ is $G_x = \{g \in G \mid g * x = x\} \leq G$.

Recalled from IA, we have the Orbit-Stabilizer Theorem. There is a bijection $\mathrm{orb}_G(x) \leftrightarrow {}^{G}/_{G_x}$, the set of left cosets in G.

In particular, if G is finite, then

$$|G| = |\mathrm{orb}_G(x)||G_x|.$$

Example. Let G be the group of all symmetries of a cube, and X be the set of vertices. Let $x \in X$ be any vertex $|\mathrm{orb}_G(x)| = 8, |G_x| = 8$. So $|G| = 48$.

Remark.
1. $\ker \phi = \cap_{x \in X} G_x$ is called the *kernel* of the group action.
2. The orbits partition X. We say that the action is *transitive* if there is just one orbit.
3. $G_{g*x} = gG_x g^{-1}$, so if $x, y \in X$ belong to the same orbit, then their stabilizers are conjugate.

Example.

1. Let G act on itself by left multiplication. That is, $g * x = gx$. The kernel of this action is
$$\{g \in G \mid g * x = x \ \forall x \in G\} = \mathbf{1}.$$
Thus, G injects into $\mathrm{Sym}(G)$. This proves,

> **Theorem 1.5 (Cayley's Theorem).** Any finite group G is isomorphic to a subgroup of S_n for some n (take $n = |G|$).

2. Let $H \leq G$, G acts on ${}^{G}\!/_{H}$, the set of left cosets, by left multiplication. That is $g * xH = gxH$.

   This action is transitive (since $(x_2 x_1^{-1}) x_1 H = x_2 H$) with
$$\begin{aligned} G_{xH} &= \{g \in G \mid gxH = xH\} \\ &= \{g \in G \mid x^{-1}gx \in H\} \\ &= xHx^{-1}. \end{aligned}$$
   Thus, $\ker(\phi) = \cap_{x \in G} xHx^{-1}$. This is the largest normal subgroup of G that is contained in H

> **Theorem 1.6.** Let G be a non-Abelian simple group, and $H \leq G$ a subgroup of index $n > 1$. Then $n \geq 5$ and G is isomorphic to a subgroup of A_n.

Proof. Let G act on $X = {}^{G}\!/_{H}$ by left coset multiplication, and let $\phi : G \to \mathrm{Sym}(X)$ be associated permutation representation.

As G is simple, $\ker(\phi) = \mathbf{1}$ or G. Since G acts transitively on X and $|X| > 1$, $\ker(\phi) = \mathbf{1}$ and $G \cong \mathrm{Im}(\phi) \leq S_n$.

Since $G \leq S_n$ and A_n is a normal subgroup of S_n. The Second Isomorphism Theorem gives $G \cap A_n \cong {}^{GA_n}\!/_{A_n} \leq {}^{S_n}\!/_{A_n} \cong C_2$. Because G is simple, we have $G \cap A_n = 1$ or G. If the intersection is trivial, we have an injection into C_2 by First Isomorphism Theorem, but G is non-Abelian. So we must have
$$G \cap A_n = G \implies G \leq A_n.$$
Finally, if $n \leq 4$, it is easy to check that A_n does not have non-Abelian simple subgroups. So we must have $n > 5$. ■

Lecture 4

27 Jan. 12:00

3. If G is a group. Let G act on itself by conjugation. That is $g * x = gxg^{-1}$. We have the following definitions.
$$\begin{aligned} \mathrm{orb}_G(x) &= \{gxg^{-1} \mid g \in G\} = \mathrm{ccl}_G(x) && \textit{(conjugacy class)} \\ G_x &= \{g \in G \mid gx = xg\} = C_G(x) \leq G && \textit{(centralizer)} \\ \ker(\phi) &= \{g \in G \mid gx = xg \ \forall x \in G\} = Z(G) \leq G. && \textit{(center)} \end{aligned}$$

Note. The map $\phi(g) : G \to G$ satisfies $h \mapsto ghg^{-1}$ is a group homomorphism, and also a bijection. That is, it is an isomorphism from G to itself.

Definition 1.13. $\mathrm{Aut}(G) = \{\text{isomorphisms } f : G \to G\}$.

Then $\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$, and $\phi : G \to \mathrm{Sym}(G)$ has image in $\mathrm{Aut}(G)$.

4. Let X be set of all subgroups of G, then G acts on X by conjugation. That is, $g * H = gHg^{-1}$.

   The stabilizer of H is $\{g \in G \mid gHg^{-1} = H = N_G(H)\}$, called the *normalizer* of H in G. This is the largest subgroup of G containing H as a normal subgroup.

   In particular $H \trianglelefteq G \iff N_G(H) = G$.

1.3 Alternating Groups

In Part IA, we showed that the elements in S_n are conjugate if and only if they have the same cycle type.

Example. In S_5, we have the following table.

Cycle type	Number of Elements	Sign
1	1	+
(* *)	10	-
(* *)(* *)	15	+
(* * *)	20	+
(* *)(* * *)	20	-
(* * * *)	30	-
(* * * * *)	24	+
Total	120	

Let $g \in A_n$. Then $C_{A_n}(g) = C_{S_n}(g) \cap A_n$. If there is an odd permutation commuting with g,

$$|C_{A_n}(g)| = \frac{1}{2}|C_{S_n}(g)| \text{ and } |\mathrm{ccl}_{A_n}(g)| = |\mathrm{ccl}_{S_n}(g)|.$$

Otherwise,

$$|C_{A_n}(g)| = |C_{S_n}(g)| \text{ and } |\mathrm{ccl}_{A_n}(g)| = \frac{1}{2}|\mathrm{ccl}_{S_n}(g)|.$$

Example. When $n = 5$, (1 2)(3 4) commutes with (1 2), and (1 2 3) commutes with (4 5). But if $h \in C_{S_5}(g)$, $g = (1\ 2\ 3\ 4\ 5)$, then

$$\begin{aligned}(1\ 2\ 3\ 4\ 5) &= h(1\ 2\ 3\ 4\ 5)h^{-1} \\ &= (h(1)\ h(2)\ h(3)\ h(4)\ h(5)),\end{aligned}$$

so $h \in \langle g \rangle \leq A_5$, and it does split. Thus, A_5 has conjugacy classes of sizes $1, 15, 20, 12, 12$.

To show the simplicity of A_5. If $H \trianglelefteq A_5$, then H is a union of conjugacy classes,

$$\implies |H| = 1 + 15a + 20b + 12c$$

with $a, b \in \{0, 1\}$ and $c \in \{0, 1, 2\}$, and by Lagrange's Theorem $|H| \mid 60$. So by simple arithmetic, $|H| = 1$ or 60. That is A_5 is simple.

Lemma 1.3. A_n is generated by 3-cycles.

Proof. Each $\sigma \in A_n$ is a product of an even number of transpositions. Thus suffices to write the product of any two transpositions as a product of 3-cycles.

We have

- $(a\ b)(b\ c) = (a\ b\ c)$,
- $(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d)$.

∎

Lemma 1.4. If $n \geq 5$, then all 3-cycles in A_n are conjugate.

Proof. We claim that every 3-cycle is conjugate to $1\ 2\ 3$. Indeed, if $(a\ b\ c) = \sigma(1\ 2\ 3)\sigma^{-1}$ for some $\sigma \in S_n$. If $\sigma \notin A_n$, then replace σ by $\sigma(4\ 5)$, and $\sigma(4\ 5)$ is an element of A_n. Note, here we use the fact that $n \geq 5$. A_4 is not simple in particular. ∎

Theorem 1.7. A_n is simple for all $n \geq 5$.

Proof. Let $1 \neq N \trianglelefteq A_n$. Suffices to show that N contains a 3-cycle, since Lemma (1.3) and (1.4) shows that we will have $N = A_n$.

Take $1 \neq \sigma \in N$ and write σ as a product of disjoint cycles. We consider three cases,

1. σ contains a cycle of length $r \geq 4$. Without loss of generality, $\sigma = (1\ 2\ 3\ \cdots\ r)\tau$. Let $\delta = (1\ 2\ 3)$, and we have

$$\begin{aligned} \sigma^{-1}\delta^{-1}\sigma\delta &= (r\ \cdots\ 2\ 1)(1\ 3\ 2)(1\ 2\ \cdots\ r)(1\ 2\ 3) \\ &= (2\ 3\ r). \end{aligned}$$

   This implies that N contains a 3-cycle.

2. σcontains two 3-cycles. Without loss of generality, let $\sigma = (1\ 2\ 3)(4\ 5\ 6)\tau$. Let $\delta = (1\ 2\ 4)$, we have

$$\begin{aligned} \sigma^{-1}\delta^{-1}\sigma\delta &= (1\ 3\ 2)(4\ 6\ 5)(1\ 4\ 2)(1\ 2\ 3)(4\ 5\ 6)(1\ 2\ 4) \\ &= (1\ 2\ 4\ 3\ 6). \end{aligned}$$

   Thus, we are done by case 1.

3. σ contains two 2-cycles. Without loss of generality, let $\sigma = (1\ 2)(3\ 4)\tau$. Let $\delta = (1\ 2\ 3)$, we have

$$\begin{aligned}\sigma^{-1}\delta^{-1}\sigma\delta &= (1\ 2)(3\ 4)(1\ 3\ 2)(1\ 2)(3\ 4)(1\ 2\ 3)\\ &= (1\ 4)(2\ 3) \equiv \pi.\end{aligned}$$

Let $\epsilon = (2\ 3\ 5)$ (here we also used $n \geq 5$), we have

$$\begin{aligned}\pi^{-1}\epsilon^{-1}\pi\epsilon &= (1\ 4)(2\ 3)(2\ 5\ 3)(1\ 4)(2\ 3)(2\ 3\ 5)\\ &= (2\ 5\ 3).\end{aligned}$$

Thus, N contains a 3-cycle.

It remains to consider σ with cycle type (* *), (* *)(* * *) which are not elements of A_n, and (* * *) which is a 3-cycle itself. ■

Lecture 5

29 Jan. 12:00

1.4 p-groups and p-subgroups

Definition 1.14. Let p be a prime. A finite group G is a p-group if $|G| = p^n, n \geq 1$.

Theorem 1.8. If G is a p-group, then $Z(G) \neq \mathbf{1}$.

Proof. For $g \in G$, we have by orbit-stabilizer theorem,

$$|\mathrm{ccl}_G(g)||C_G(g)| = |G| = p^n.$$

So each conjugacy class has size a power of p. Since G is a disjoint union of conjugacy classes, $|G| = \#(\text{conjugacy classes of size } 1) \mod p$. It is easy to see that the conjugacy classes of size 1 are precisely the elements in the center of a group. That is, $|Z(G)| \equiv 0 \mod p$, and hence $Z(G) \neq \mathbf{1}$. ■

Corollary 1.1. The only simple p-group is C_p.

Proof. Let G be a simple p-group. Since $Z(G) \trianglelefteq G$, we have $Z(G) \neq \mathbf{1}$, so $Z(G) = G$. That is G is Abelian. We know that the only Abelian simple groups are C_p, so $G = C_p$. ■

Corollary 1.2. Let G be a p-group of order p^n. Then G has a subgroup of order p^r for all $0 < r \leq n$.

Proof. By Lemma (1.2), G has a composition series

$$\mathbf{1} \cong G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_m \cong G$$

with each quotient ${}^{G_{i+1}}/_{G_i}$ simple.

Because G is a p-group, each of the quotients is a p-group. So ${}^{G_{i+1}}/_{G_i} \cong C_p$.

Thus, $|G_i| = p^i$ for $0 \leq i \leq m = n$. ∎

Lemma 1.5. For G a group, if ${}^{G}/_{Z(G)}$ is cyclic, then G is Abelian. (so in fact ${}^{G}/_{Z(G)} = \mathbf{1}$)

Proof. Let $gZ(G)$ be a generator for ${}^{G}/_{Z(G)}$, then each coset is of the form $g^{r Z(G)}$ for some $r \in \mathbb{Z}$.

Thus, $G = \{g^r z \mid r \in \mathbb{Z}, z \in Z(G)\}$. We check that two general elements in the group commute.

$$g^{r_1} z_1 g^{r_2} z_2 = g^{r_1 + r_2} z_1 z_2 = g^{r_1 + r_2} z_2 z_1 = g^{r_2} z_2 g^{r_1} z_1.$$

So G is Abelian. ∎

Corollary 1.3. If $|G| = p^2$ then G is Abelian.

Proof. We have three choices for the size of the center of the group. Noting that the center cannot be trivial for a p-group. So $|Z(G)| = p$ or $|Z(G)| = p^2$.

If $|Z(G)| = p$, $|{}^{G}/_{Z(G)}| = p$, apply Lemma (1.5), and we have a contradiction.

If $|Z(G)| = p^2$, then $Z(G) = G$ so G is Abelian. ∎

Note that this is not true for $|G| = p^3$.

Theorem 1.9 (Sylow Theorems). Let G be a finite group of order $p^a m$ where p is a prime with $p \nmid m$. Then

1. The set $\mathrm{Syl}_p(G) = \{P \leq G \mid |P| = p^a\}$ of Sylow p-subgroups is non-empty.
2. All elements of $\mathrm{Syl}_p(G)$ are conjugates.
3. If $n_p := \left|\mathrm{Syl}_p(G)\right|$ satisfies $n_p \equiv 1 \mod p$ and $n_p \mid |G|$ (and so $n_p \mid m$).

Corollary 1.4. If $n_p = 1$, then the unique Sylow p-subgroup is normal.

It is useful to show that the group of a certain order cannot be simple.

Proof. Let $g \in G$, and $P \in \mathrm{Syl}_p(G)$. Then $gPg^{-1} = P$ because $n_p = 1$. Thus, $P \trianglelefteq G$. ∎

Example. Let $|G| = 1000 = 2^3 \cdot 5^3$. Then $n_5 \equiv 1 \mod 5$ and $n_5 \mid 8$. So $n_5 = 1$. Thus, the unique Sylow 5-subgroup is normal and of order 125. Hence, G is not simple.

Example. Let $|G| = 132 = 2^2 \cdot 3 \cdot 11$. We have $n_{11} \equiv 1 \mod 11$ and $n_{11} \mid 12$, so $n_{11} = 1$ or 12.

Suppose that G is simple. Then $n_{11} \neq 1$ (otherwise the Sylow 11-subgroup is normal) and hence $n_{11} = 12$.

Now we consider $n_3 \equiv 1 \mod 3$ and $n_3 \mid 44$. So $n_3 = 1, 4, 22$. Similarly, $n_3 \neq 1$.

Suppose $n_3 = 4$. Then letting G act on $\mathrm{Syl}_3(G)$ by conjugation gives a group homomorphism $\phi : G \to S_4$. So $\ker(\phi) \trianglelefteq G \implies \ker(\phi) = 1$ or G. But by second Sylow Theorem, the action is transitive, so the kernel must be trivial, but $132 > 24$, so ϕ cannot possibly be an injection.

Thus, $n_3 = 22$ and $n_{11=12}$. So G would have $22 \cdot (3-1)$ elements of order 3 and G has $12 \cdot (11-1) = 120$ elements of order 11. But $44 + 120 > 132 = |G|$, contradiction.

Proof of Sylow Theorems. We have $|G| = p^a m$ where p is prime and $p \nmid m$.

1. Let Ω be set of all subsets of G of order p^a. So

   $$|\Omega| = \binom{p^a m}{p^a} = \frac{p^a m}{p^a} \frac{p^a m - 1}{p^a - 1} \cdots \frac{p^a m - p^a + 1}{1}$$

   for $0 \leq k < p^a$, the number $p^a m - k$, the numbers $p^a m - k$ and $p^a - k$ are divisible by the same powers of p. So $|\Omega|$ is coprime to p. Let G act on $|\Omega|$ by left multiplication. That is, for $g \in G$ and $X \in \Omega$,

   $$g * X = \{gx \mid x \in X\} \in \Omega.$$

   For any $X \in \Omega$, we have

   $$|G_X||\mathrm{orb}_G(X)| = |G| = p^a m.$$

   Because $|\Omega|$ is coprime to p. We can find some X such that $|\mathrm{orb}_G(X)|$ is coprime to p. Thus, $p^a \mid |G_X|$.

   On the other hand, if $g \in G$ and $x \in X$, then $g \in (gx^{-1}) * X$, and we have

   $$G = \bigcup_{g \in G} g * X = \bigcup_{y \in \mathrm{orb}_G(x)} y.$$

   So $|G| \leq |\mathrm{orb}_G(X)||X| \implies |G_x| = \frac{|G|}{|\mathrm{orb}_G(X)|} \leq |X| = p^a$.

   Combining the two facts, we have $|G_X| = p^a$, i.e., $G_x \in \mathrm{Syl}_p(G)$.

2. We prove a stronger result.

   Lemma 1.6. If $P \in \mathrm{Syl}_p(G)$ and $Q \leq G$ is a p-subgroup, then $Q \leq gPg^{-1}$ for some $g \in G$.

The lemma implies Second Sylow Theorem by taking Q a Sylow subgroup.

Let Q act at the set of left cosets ${}^{G}/_{P}$ by left multiplication. That is, $q * gP = (qg)P$. By orbit-stabilizer Theorem, each orbit has size dividing $|Q|$, so each orbit has size 1 or a power of p.

Since $|{}^{G}/_{P}| = m$ is coprime to p, there must exist an orbit of size 1. That is, there exists $g \in G$ such that $qgP = gP$ for all q. So $g^{-1}qg \in P$ for all $q \in Q$. So $Q \leq gPg^{-1}$.

3. Let G act on $\mathrm{Syl}_p(G)$ by conjugation. By Second Sylow Theorem, the action is transitive. Thus, orbit-stabilizer implies $n_p = \left|\mathrm{Syl}_p(G)\right| \mid |G|$.

   Now let $P \in \mathrm{Syl}_p(G)$. Then P act on $\mathrm{Syl}_p(G)$ by conjugation. The orbits have size dividing $|P| = p^a$, the size is either 1 or a power of p. So P is in an orbit of size 1.

   To show $n_p \equiv 1 \mod p$, suffices to show that $\{P\}$ is the only orbit of size one. If $\{Q\}$ is another orbit of size 1, then P normalizes Q. That is $P \leq N_G(Q)$. Note that P, Q are both Sylow p-subgroups of $N_G(Q)$.

   Thus, by Second Sylow Theorem, P and Q are conjugate in $N_G(Q)$, hence equal since $Q \trianglelefteq N_G(Q)$. Hence, $P = Q$ and $\{P\}$ is the unique orbit of size 1.

■

Lecture 6

1 Feb. 2022

1.5 Matrix Groups

For F a field (e.g. $\mathbb{C}$ or ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$), Let $GL_n(G)$ be the $n \times n$ invertible matrices with entries in F. And let $SL_n(G) = \ker(\det)$.

Let $Z \trianglelefteq GL_n(F)$ be subgroup of scalar matrices.

Definition 1.15. The *projective general linear group* is

$$PGL_n(F) = {}^{GL_n(F)}/_{Z},$$

and the *projective special linear group* is

$$PSL_n(G) = {}^{SL_n(F)}/_{Z \cap SL_n(F)} \cong {}^{Z \cdot SL_n(F)}/_{Z} \leq PGL_n(F).$$

Example. Consider $G = GL_n({}^{\mathbb{Z}}/_{p\mathbb{Z}})$. A list of n vectors in $({}^{\mathbb{Z}}/_{p\mathbb{Z}})^n$ are the columns of some $A \in G$ if and only if they are linearly independent. Thus,

$$\begin{aligned} |G| &= (p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1}) \\ &= p^{1+2+\cdots+n-1}(p^n - 1)(p^{n-1} - 1) \cdots (p - 1) \\ &= p^{\binom{n}{2}} \prod_{i=1}^{n} (p^i - 1). \end{aligned}$$

So the Sylow p-subgroups have sizes $p^{\binom{n}{2}}$. Let

$$U = \left\{ \begin{pmatrix} 1 & * & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\} \leq G,$$

the set of upper triangular matrices with 1 on the diagonal. Then $U \in \mathrm{Syl}_p(G)$, since we have $\binom{n}{2}$ entries in U, and each can take p values.

The group $PGL_2(\mathbb{C})$ acts on $\mathbb{C} \cup \{\infty\}$ via Möbius transformations, and similarly, $PGL_2(\mathbb{Z}/p\mathbb{Z})$ acts on $\mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$ via the finite field equivalent of Möbius transformation.

Since the scalar matrices act trivially, we obtain an action of $PGL_2(\mathbb{Z}/p\mathbb{Z})$.

Lemma 1.7. The permutation representation $PGL_2(\mathbb{Z}/p\mathbb{Z}) \to S_{p+1}$ is injective (in fact in isomorphism if $p = 2$ or $p = 3$).

Proof. Suppose $\frac{az+b}{cz+d} = z$ for all $z \in \mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$. Setting $z = 0$ gives $b = 0$. Setting $z = \infty$ gives $c = 0$. And setting $z = 1$ gives $a = d$. So it must be a scalar matrix, hence trivial in $PGL_2(\mathbb{Z}/p\mathbb{Z})$. The isomorphism can be established by considering the sizes of the groups when $p = 2$ and $p = 3$. ∎

Lecture 7

3 Feb. 2022

Lemma 1.8. If p is an odd prime

$$|PSL_2(\mathbb{Z}/p\mathbb{Z})| = \frac{p(p-1)(p+1)}{2}.$$

Proof. From above, $|GL_2(\mathbb{Z}/p\mathbb{Z})| = p(p^2-1)(p-1)$. First we note the group homomorphism $GL_2(\mathbb{Z}/p\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})^\times$ by taking the determinant is surjective. Thus, $|SL_2(\mathbb{Z}/p\mathbb{Z})| = \frac{|GL_2(\mathbb{Z}/p\mathbb{Z})|}{p-1} = p(p-1)(p+1)$.

And if a scalar matrix $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \in SL_2(\mathbb{Z}/p\mathbb{Z})$, then $\lambda^2 \equiv 1 \mod p$, so

$$p \mid (\lambda - 1)(\lambda + 1) \implies \lambda \equiv \pm 1 \mod p.$$

Thus, $Z \cap SL_2(\mathbb{Z}/p\mathbb{Z}) = \{\pm I\}$, and they are distinct since $p > 2$. So we have

$$|PSL_2(\mathbb{Z}/p\mathbb{Z})| = \frac{|SL_2(\mathbb{Z}/p\mathbb{Z})|}{2} = \frac{p(p-1)(p+1)}{2}.$$

∎

Example. Let $G = PSL_2(\mathbb{Z}/5\mathbb{Z})$, then $|G| = \frac{4 \cdot 5 \cdot 6}{2} = 60$.

Let G act on $\mathbb{Z}/5\mathbb{Z} \cup \{\infty\}$ via the Möbius-like transformation. By Lemma (1.7), the permutation representation $\phi : G \to \mathrm{Sym}(\{0,1,2,3,4,\infty\})$ is injective. We claim that $\mathrm{Im}(\phi) \leq A_6$; that is, $\psi : G \to S_6 \to \{\pm 1\}$ is trivial.

Let $h \in G$ have order $2^n m$, m odd. If $\psi(h^m) = 1$, then

$$\psi(h)^m = 1 \implies \psi(h) = 1.$$

Noting that h^m has order 2^n, it suffices to show that $\psi(g) = 1$ for all $g \in G$ or order a power of 2. By Lemma (1.6), every such g belongs to a Sylow 2-subgroup.

It suffices to show that $\psi(H) = 1$ for H a particular Sylow 2-subgroup. (since $\ker(\psi)$ is normal and all Sylow subgroups are conjugate)

Take $H = \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle \leq G$. We compute $\phi\left(\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}\right) = (1\ 4)(2\ 3)$ and $\phi\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = (0\ \infty)(1\ 4)$. Both of which are even permutations. Thus, $\psi(H) = 1$, and this proves the claim.

Lastly, by example sheet Q14 tells you if $G \leq A_6$ and $|G| = 60$ then $G \cong A_5$.

Property (not proved in the course).

1. $PSL_n(\mathbb{Z}/p\mathbb{Z})$ is a simple group for all $n \geq 2$ and p a prime except when $(n, p) = (2, 2), (2, 3)$. (finite groups of Lie type)
2. The smallest non-Abelian simple groups are $A_5 \cong PSL_2(\mathbb{Z}/5\mathbb{Z})$ of order 60 and $PSL_2(\mathbb{Z}/7\mathbb{Z}) \cong GL_3(\mathbb{Z}/2\mathbb{Z})$ of order 168.

1.6 Finite Abelian groups

Later in the course we will prove the following result.

Theorem 1.10. Every finite Abelian group is isomorphic to a product of cyclic groups.

Note. Such an isomorphism is not unique.

Lemma 1.9. If $m, n \in \mathbb{Z}_{\geq 1}$ coprime, then $C_m \times C_n \cong C_{mn}$.

Proof. Let g and h be generators of C_n and C_m. Then $(g, h) \in C_m \times C_n$ and $(g, h)^r = (g^r, h^r)$. Hence, $(g, h)^r = 1 \iff m \mid r \wedge n \mid r \iff mn \mid r$. Thus, (g, h) has order $mn = |C_m \times C_n|$. And we have $C_m \times C_n \cong C_{mn} = \langle (g, h) \rangle$. ■

Corollary 1.5. Let G be a finite Abelian group, then $G \cong C_{n_1} \times C_{n_2} \times \cdots C_{n_k}$ where n_i is a prime power.

Proof. If $n = p_1^{a_1} \cdots p_r^{a_r}$ ($p_1, \ldots, p_r$ distinct primes), then Lemma (1.5) shows $C_n \cong C_{p_1^{a_1}} \times \cdots C_{p_r^{a_r}}$. Writing each of the cyclic groups in Theorem (1.10) in this way gives the result. ■

We will prove a refinement of Theorem (1.10).

Theorem 1.11. Let G be a finite Abelian group. Then

$$G \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_t}$$

for some $d_1 \mid d_2 \mid \cdots \mid d_t$.

Remark. The integers $n_1, \ldots, n_k$ in Corollary (1.5) (up to order) and $d_1, \ldots, d_t$ in Theorem (1.11) (assuming $d_1 > 1$) are uniquely determined by G. (Proof omit)

Example.

1. The Abelian groups of order 8 are C_8, $C_2 \times C_4$, $C_2 \times C_2 \times C_2$.
2. The Abelian groups of order 12 are $C_2 \times C_2 \times C_3$ and $C_4 \times C_3$ by Theorem (1.5), and $C_2 \times C_6$ and C_{12} by Theorem (1.11).

Definition 1.16. The *exponent* of a group G is the least integer $n \geq 1$ such that $g^n = 1\ \forall g \in G$. That is, the lcm of all the orders of the elements of G.

Example. A_4 has exponent 6. The exponent here is greater than the biggest order of an element of the group.

Corollary 1.6. Every finite Abelian group contains an element whose order is the exponent of the group.

Proof. If $G \cong C_{d_1} \times \cdots \times C_{d_t}$ with $d_1 \mid d_2 \mid \cdots \mid d_t$, then every $g \in G$ has order dividing d_t, and if $h \in C_{d_t}$ is a generator, then $(1, \ldots, h) \in G$ has order d_t. Thus, G has exponent d_t. ■

Lecture 8

5 Feb. 2022

2 Rings

2.1 Definitions and Examples

Definition 2.1. A *ring* is a triple $(R, +, \cdot)$ consisting of a set R and two binary operations $+ : R \times R \to R$ and $\cdot : R \times R \to R$ satisfying the following axioms:

1. $R, +$ is an Abelian group with identity $0 = 0_R$.
2. Multiplication is associative and has an identity. i.e.

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \;\forall x, y, z \in R$$

and

$$\exists 1 = 1_R \in R \text{ s.t. } x \cdot 1 = 1 \cdot x = x \;\forall x \in R.$$

We say R is a *commutative* ring if $x \cdot y = y \cdot x \;\forall x, y \in R$. In fact, in this course, we will only consider commutative rings.

3. Distributivity: $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$ for all $x, y, z \in R$.

Remark.

1. As in case of groups, we need to check closure.
2. For $x \in R$, we write $-R$ as the inverse of x under $+$, and abbreviate $x + (-y)$ as $x - y$.
3. $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x \implies 0 \cdot x = 0 \quad \forall x \in R$.
4. $$\begin{aligned} 0 = 0 \cdot x &= (1 - 1) \cdot x \\ &= 1 \cdot x + (-1) \cdot x \\ &= x + (-1) \cdot x \\ \implies (-1) \cdot x &= -x \quad \forall x \in R. \end{aligned}$$

Definition 2.2. A subset $S \subseteq R$ is a *subring* (written $S \leq R$) if it is a ring under $+$ and $\cdot$, with the same identity elements 0 and 1.

Example.

1. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.
2. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \leq \mathbb{C}$ (ring of Gaussian integers).
3. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \leq \mathbb{R}$.
4. $\mathbb{Z}/n\mathbb{Z} = \{\text{integers mod } n\}$.
5. If R, S are rings, the ring $R \times S$ is a ring via the operations
   - $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$;
   - $(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$;
   - $0_{R \times S} = (0_R, 0_S)$ and $1_{R \times S} = (1_R, 1_S)$.

   (Note: $R \times \{0\}$ is not a subring).

6. If R is a ring, a polynomial f over R is an expression $f = a_0 + a_1 X + a_2 X^2 + \cdot + a_n X^n, a_i \in R$. "$X$" is just a formal symbol.

   The degree of a polynomial is largest $n \in \mathbb{N}$ such that a_n is nonzero. We write $R[X]$ for the set of all polynomials over R.

   If $g = b_0 + b_1 X + \cdots + b_m X^m$ is another polynomial, set

$$f + g = \sum_i (a_i + b_i) X^i,$$

$$f \cdot g = \sum_i (\sum_{j=0}^{i} a_j b_{i-j}) X^i.$$

   Then $R[X]$ is a ring with identities 0_R and 1_R which are constant polynomials.

   We can identify R with subring of $R[X]$ of constant polynomials (i.e. $\sum_i a_i X^i, a_i = 0\ \forall i > 0$).

Definition 2.3. An element $r \in R$ is a *unit* if it has an inverse under multiplication, i.e. $\exists s \in R$ s.t. $s \cdot r = 1$.

The units in R form a group $(R^\times, \cdot)$ under multiplication.

Example.

- $\mathbb{Z}^\times = \{\pm 1\}$.
- $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$

Definition 2.4. A *field* is a ring with $0 \neq 1$, such that every non-zero element is a unit.

Example. $\mathbb{Q}$, $\mathbb{Z}/p\mathbb{Z}$ with p prime.

Remark. If R is a ring with $0 = 1$, then $x = 1 \cdot x = 0 \cdot x = 0$ for all $x \in R$. And $R = \{0\}$ is the *trivial ring*.

Proposition 2.1. Let $f, g \in R[X]$. Suppose the leading coefficient of g is a unit. Then there exist $q, r \in R[X]$ such that

$$f(x) = q(x) g(x) + r(x) \text{ where } \deg(r) < \deg(g).$$

Proof. Induction on $n = \deg(f)$. Write

$$\begin{aligned} f(X) &= a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0, & a_n &\neq 0 \\ g(X) &= b_m X^m + b_{m-1} X^{m-1} + \cdots + b_0. & b_m &\in R^\times \end{aligned}$$

If $n < m$, then put $q = 0, r = f$, and we are done.

Otherwise, we have $n \geq m$, and we set

$$f_1(X) = f(X) - a_n b_m^{-1} g(X) X^{n-m}$$

because b_m is a unit. The coefficient of X^n is $a_n - a_n b_m^{-1} b_m = 0$. Thus, $\deg(f_1) < n$. By inductive hypothesis $\exists q_1, r \in R[X]$ such that

$$f_1(X) = q_1(X) g(X) + r(X), \text{ where } \deg(r) < \deg(g).$$

Therefore,

$$f(X) = (q_1(X) + a_n b_m^{-1} X^{n-m}) g(X) + r(X).$$

■

Remark. We often work with polynomials over a field, then we only need the assumption that $g \neq 0$.

Example.

1. If R is a ring and X a set, then the set of all functions $X \to R$ is a ring under point-wise operations. That is,

$$(f+g)(x) = f(x) + g(x);$$
$$(f \cdot g)(x) = f(x) \cdot g(x).$$

   More interesting examples will appear as subrings. For example, the continuous functions from $\mathbb{R} \to \mathbb{R}$ and the polynomial functions $\mathbb{R} \to \mathbb{R}$ which is $\mathbb{R}[X]$.

2. Power series ring. $R[\![X]\!] = \{a_0 + a_1 X + a_2 X^2 + \cdots \mid a_i \in \mathbb{R}\}$ with the same operation as the polynomial. (you should not think this as infinite sum of elements, but a formal object instead)

3. Laurent polynomials.

$$R[X, X^{-1}] = \{\sum_{i \in \mathbb{Z}} a_i X^i \mid a_i \in R, a_i \text{ is non-zero for finitely many } i\}.$$

Lecture 9

8 Feb. 2022

2.2 Homomorphisms, Ideals and Quotients

Definition 2.5. Let R and S be rings. A function $\phi : R \to S$ is a *ring homomorphism* if

1. $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) \quad \forall r_1, r_2 \in R$,
2. $\phi(r_1 \cdot r_1) = \phi(r_1) \cdot \phi(r_2) \quad \forall r_1, r_2 \in R$,
3. $\phi(1_R) = 1_S$.

A ring homomorphism that is also a bijection is called an *isomorphism*.

The *kernel* of ϕ is $\ker(\phi) = \{r \in R \mid \phi(r) = 0_S\}$.

Lemma 2.1. A ring homomorphism $\phi : R \to S$ is injective if and only if $\ker(\phi) = \{0_R\}$.

Proof. $\phi : (R, +) \to (S, +)$ is also a group homomorphism. And the result follows from the corresponding result from groups. ■

Definition 2.6. A subset $I \subseteq R$ is an *ideal*, written $I \trianglelefteq R$, if

1. I is a subgroup of $(R, +)$;
2. if $r \in R$ and $x \in I$, then $rx \in I$.

We say I is *proper* if $I \neq R$.

Lemma 2.2. If $\phi : R \to S$ is a ring homomorphism, then $\ker(\phi)$ is an ideal of R.

Proof. Again, $\phi : (R, +) \to (S, +)$ is a group homomorphism between the additive groups. So $\ker(\phi)$ is a subgroup of $(R, +)$.

If $r \in R$ and $x \in \ker(\phi)$, then

$$\phi(rx) = \phi(r)\phi(x) = \phi(r) \cdot 0_S = 0_S \implies rx \in \ker(\phi).$$

■

Remark. If I contains a unit, then $1_R \in I$ because ideal is closed by multiplication with any element in R; hence, $I = R$. Thus, if I is a proper ideal, $1_R \notin I$, so I is not a subring of R.

Lemma 2.3. The ideals in $\mathbb{Z}$ are $n\mathbb{Z} = \{\dots, -2n, -n, 0, n, 2n, \dots\}$, for $n = 0, 1, 2, \dots$.

Proof. Certainly, $n\mathbb{Z} \trianglelefteq \mathbb{Z}$.

Let $I \trianglelefteq \mathbb{Z}$ be a non-zero ideal, and let n be the smallest positive integer in I. Then $n\mathbb{Z} \subseteq I$. If $m \in I$, then write $m = qn + r$ where $q, r \in \mathbb{Z}$, and $0 \leq r < n$ by division algorithm. Then $r = m - qn \in I$ contradicts the minimality of n unless $r = 0$. Then we have $m \in n\mathbb{Z}$; i.e. $I = n\mathbb{Z}$. ■

Definition 2.7. For $a \in R$, write $(a) = \{ra \mid r \in R\} \trianglelefteq R$. This is the *ideal generated by a*.

Generally, if $a_1, \dots, a_n \in R$, we write *the ideal generated by* $a_1, \dots, a_n$ as

$$(a_1, \dots, a_n) = \{r_1 a_1 + r_2 a_2 + \ldots + r_n a_n \mid r_i \in R\} \trianglelefteq R.$$

Definition 2.8. Let $I \trianglelefteq R$, we say I is *principal* if $I = (u)$ for some $u \in R$.

Theorem 2.1. If $I \trianglelefteq R$, then the set ${}^{R}/_{I}$ of cosets of I in $(R, +)$ forms a ring (called the *quotient ring*) with the operations

$$\begin{aligned}(r_1 + I) + (r_2 + I) &= r_1 + r_2 + I,\\ (r_1 + I) \cdot (r_2 + I) &= r_1 \cdot r_2 + I\end{aligned}$$

and $0_{R/I} = O_R + I$, $1_{R/I} = 1_R + I$.

Moreover, the map $R \to {}^{R}/_{I}, r \mapsto r + I$ is a ring homomorphism (called the *quotient map*) with kernel I.

Proof. We already know that $({}^{R}/_{I}, +)$ is a group. We want to show that the multiplication is well-defined. If $r_1 + I = r_1' + I$, $r_2 + I = r_2' + I$, then for some $a_1, a_2 \in I$, $r_1' = r_1 + a_1$, $r_2' = r_2 + a_2$. Then we have

$$\begin{aligned}r_1' r_2' &= (r_1 + a_1)(r_2 + a_2)\\ &= r_{1r_2 + r_1} a_2 + r_2 a_1 + a_1 a_2.\end{aligned}$$

Thus, $r_1 r_2 + I = r_1' r_2' + I$.

The remaining properties for ${}^{R}/_{I}$ follows from those properties for R. And the quotient map is clearly a ring homomorphism from the definitions of the quotient ring. ■

Example.

1. $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ with quotient ring ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$. To be precise, ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$ has elements $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots$. Addition and multiplication are carried out $\bmod n$.

2. Consider $(X) \trianglelefteq \mathbb{C}[X]$, the polynomials with constant term 0.

   If $f(X) = a_n X^n + \cdots + a_1 X + a_0, a_i \in \mathbb{C}$, then $f(X) + (X) = a_0 + (X)$. There is a bijection from ${}^{\mathbb{C}[X]}/_{(X)} \to \mathbb{C}, f(X) + (X) \mapsto f(0)$.

   These maps are ring homomorphisms. Thurs, ${}^{\|C[X]}/_{(X)} \cong \mathbb{C}$.

3. Consider $(X^2 + 1) \trianglelefteq \mathbb{R}[X]$,

   $${}^{\mathbb{R}[X]}/_{(X^2+1)} = \{f(X) + (X^2 + 1) \mid f(X) \in \mathbb{R}[X]\}.$$

   By Proposition (2.1), $f(X) = q(X)(X^2 + 1) + r(X)$ with $\deg r < 2$, i.e. $r(X) = a + bX, a, b \in \mathbb{R}$. Thus,

   $${}^{mathbbR}/_{(X^2+1)} = \{a + bX + (X^2 + 1) \mid a, b \in \mathbb{R}\}.$$

   If $a + bX + (X^2 + 1) = a' + b'X + (X^2 + 1)$, then

   $$a - a' + (b - b')X = g(X)(X^2 + 1).$$

Comparing degrees, we see $g(x) = 0$ and $a = a'$ and $b = b'$. Consider the bijection

$$\begin{aligned} \phi\colon {}^{\mathbb{R}[X]}\!/_{X^2+1} &\longrightarrow \mathbb{C} \\ a + bX + (X^2+1) &\longmapsto a + bi. \end{aligned}$$

We show that ϕ is a ring homomorphism. It preserves addition and maps $1 + (X^2+1)$ to 1.

$$\phi(a + bX + (X^2+1))\phi(c + dX + (X^2+1))$$