Modern Algebra I

Sungchan Yi

Spring 2023

Part I

Groups and Subgroups

Introduction

Section 1. Introduction and Examples

수 체계의 확장.

$$\mathbb{N} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{R} \longrightarrow \mathbb{C}$$

학부 현대대수학의 최종 목표는 다음 정리를 증명하는 것.

Theorem. n차 방정식의 일반해는 존재하지 않는다. ($n \geq 5$)

March 6th, 2023

추상적인 개념을 공부하는 이유는 구체적인 example 때문이다. Example이 곧 motivation이 되기 때문이다.[1]

- Complex numbers $\mathbb{C}$. $a + bi \in \mathbb{C}$, $a, b \in \mathbb{R}$ and $+, \times$ defined on them.
- The unit circle $U = \{a + bi : a^2 + b^2 = 1, a, b \in \mathbb{R}\} = \{e^{i\theta} : 0 \leq \theta < 2\pi\}$. U is not closed under addition, but closed under multiplication.

  Note that the above two representations are intrinsically the 'same' representations of the unit circle. We write

  $$(U, \cdot) \approx \big([0, 2\pi), +_{2\pi}\big)$$

  and say that these two are **isomorphic**.

[1] 이인석 교수님: 추상화는 구체적인 example이 없으면 의미 없다.

- **Roots of Unity**: $U_n = \{\xi \in \mathbb{C} : \xi^n = 1\}$. We can see that

$$\xi_k = e^{\frac{2\pi k}{n}i}, \quad (k = 0, \ldots, n-1).$$

When we multiply two elements for example, we do the following.

$$\xi_1 \cdot \xi_2 = e^{\frac{2\pi}{n}i} \cdot e^{\frac{4\pi}{n}i} = e^{\frac{6\pi}{n}i} = \xi_3$$

If we look closely, we see that we have transformed elements of $(U, \cdot)$ to $\big([0, 2\pi), +_{2\pi}\big)$. This can be done because the two sets are **isomorphic**!

March 8th, 2023

Definition. (Binary Operation) A **binary operation** $*$ on a set S is defined as a function

$$* : S \times S \to S$$

We write $a * b$ instead of $*(a, b)$.

Remark. If you consider the number systems like $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, we already know operations defined on them. We are just naming them *binary operations*. The examples came first, and the definitions came afterwards. We can also see that the definitions are really useful, and it will serve as a tool for formalizing our theory.

Example. Examples of binary operations.

(1) Addition $+$ and multiplication $\cdot$ on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(2) Subtraction $-$ is not a binary operation on $\mathbb{N}$. We extend $\mathbb{N}$ to $\mathbb{Z}$, so that $-$ is a binary operation on $\mathbb{Z}$.

(3) The set of functions $f : \mathbb{R} \to \mathbb{R}$, and $+, -, \times, \circ$ defined on it.

Definition. (Closure) For a set S and a binary operation $*$ on S, suppose that $H \subset S$. We restrict the domain of $*$ to $H \times H$. Then

$$* |_{H \times H} : H \times H \to S.$$

If the image of $* |_{H \times H} \subset H$, then we say that H **is closed under** $*$.

Remark. When we learn new definitions, it's very important to think about examples that we already know. Often books give trivial examples first, and then show some non-trivial examples, motivating us to study. Books are written in that way!

Definition. Let $(S, *)$ be given. We say that

(1) $*$ is **commutative** if $a * b = b * a$ for all $a, b \in S$.

(2) $*$ is **associative** if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

Example. Consider these binary operations on $\mathbb{Z}$.

(1) $a * b = a$, $*$ is not commutative but associative.

(2) $a * b = a + 2$, $*$ is not commutative nor associative.

Remark. To study these binary operations, we first start with finite sets where we can write tables with the results of the binary operation.

$$S = \{a\} \implies \begin{array}{c|c} * & a \\ \hline a & a \end{array}, \qquad S = \{a, b\} \implies \begin{array}{c|c|c} * & a & b \\ \hline a & & a * b \\ \hline b & b * a & \end{array}$$

Consider the relation between binary operation on a finite set S and tables. Binary operation is a function, so we have the existence and uniqueness of $a * b$. In terms of tables, we see that each cell in the table should have a value and it should be uniquely determined. So we conclude that *we can describe a binary operation with a table.*

March 13th, 2023

Section 3. Isomorphic Binary Structures

Consider $S = \{a, b, c\}, S' = \{1, 2, 3\}$ and binary operations $*, *'$, defined as the following.

$*$	a	b	c
a	b	a	c
b	c	a	b
c	a	b	c

$*'$	1	2	3
1	2	1	3
2	3	1	2
3	1	2	3

We see that if we rename a, b, c to $1, 2, 3$ respectively, we see that the tables are actually *equivalent*. How do we formalize the notion of equivalence of binary structures $(S, *), (S', *')$?

Definition. (Isomorphism) Let $(S, *)$ and $(S', *')$ be binary structures. If there exists a bijection $\varphi : S \to S'$ such that

$$\varphi(a * b) = \varphi(a) *' \varphi(b), \quad \forall a, b \in S,$$

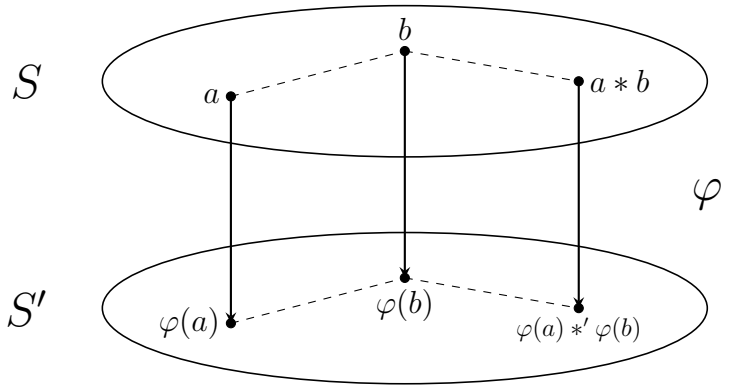
then φ is called an **isomorphism** between $(S, *)$ and $(S', *')$. We say that $(S, *)$ and $(S', *')$ are **isomorphic** to each other.

Definition. (Homomorphism) Let $(S, *)$ and $(S', *')$ be binary structures. A map $\varphi : S \to S'$ such that

$$\varphi(a * b) = \varphi(a) *' \varphi(b), \quad \forall a, b \in S$$

is called a **homomorphism** between $(S, *)$ and $(S', *')$.

Remark. Isomorphisms are *renaming functions* that preserve the structure of a set. Isomorphisms are homomorphisms that are bijective. Also, homomorphisms can be seen as a somewhat confusing(?) renaming functions, since they aren't bijective.



Example. Examples of isomorphisms.

(1) Let $\varphi : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ with $\varphi(x) = e^x$ for $x \in \mathbb{R}$.

(2) Let $\varphi : (\mathbb{Z}, +) \to (2\mathbb{Z}, +)$ with $\varphi(n) = 2n$ for $n \in \mathbb{Z}$.

(3) Non-example: $(\mathbb{Z}, *) \not\cong (\mathbb{R}, *)$ (different cardinality)

Remark. Structural properties: properties preserved by isomorphisms

(1) Number of elements (cardinality, for infinite sets)

(2) Commutativity, associativity

(3) The equation $a * x = b$, $\forall a, b \in S$ has a solution in S

We can disprove the existence of an isomorphism by showing that any of the structural properties do not hold.

Example. For $(\mathbb{Z}, \cdot)$ and $(\mathbb{Z}^+, \cdot)$ we want to show that these two are not isomoprhic. Consider the equation $x^2 = x$. In $\mathbb{Z}$, the solutions are $x = 0, 1$, but in $\mathbb{Z}^+$, the solution is unique, $x = 1$.

Proof. Suppose that $\mathbb{Z}$ and $\mathbb{Z}^+$ are isomorphic, and let φ be the isomorphism. Let $\varphi(0) = a$, $\varphi(1) = b$. Then $a \neq b$, since φ is a bijection. However,

$$a = \varphi(0 \cdot 0) = \varphi(0) \cdot \varphi(0) = a \cdot a, \quad b = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) = b \cdot b$$

but in $\mathbb{Z}^+$ there is only one solution to $x^2 = x$. This is a contradiction, so φ is not an isomorphism.

Definition. (Identity) Let $(S, *)$ be a binary structure. If $e \in S$ satisfies

$$e * a = a * e = a, \quad \forall a \in S,$$

then e is called the **identity** element of S.

Theorem. Identities are unique, if it exists.

Proof. Let $e, e' \in S$ be identities of S. Then,

$$e = e * e' = e' * e = e'$$

so $e = e'$.

Theorem. If $\varphi : S \to S'$ is an isomorphism, φ maps the identity to the identity.

Proof. Let $e \in S$ be the identity of S. For any $t \in S'$, there exists $s \in S$ such that $\varphi(s) = t$. Then

$$t *' \varphi(e) = \varphi(s * e) = \varphi(s) = t, \quad \varphi(e) *' t = \varphi(e * s) = \varphi(s) = t,$$

so $\varphi(e)$ is the identity of S'.

March 15th, 2023

Section 4. Groups

Definition. (Inverse) Let $(S, *)$ be a binary structure with identity $e \in S$. If $x \in S$ satisfies

$$a * x = x * a = e \text{ for some } a \in S,$$

then x is an **inverse** of a, and we write $x = a^{-1}$.

Definition. (Group) Let $(G, *)$ be a binary structure, with the following properties.

(1) $*$ is associative.

(2) G has an identity element.

(3) For all $x \in G$, there exists an inverse of x in G.

Then $G = (G, *)$ is called a **group**.

$(\mathbb{N}, +)$ is not a group. The equation $n+x = m$, $(n, m \in \mathbb{N})$ does not have a solution if $n \leq m$. So we extend the number system to $\mathbb{Z}$ and consider $n + x = m$ for $n, m \in \mathbb{Z}$. This equation always has a solution, this is due to the fact that $(\mathbb{Z}, +)$ is a group. The operation $+$ is associative, $\mathbb{Z}$ has an identity 0, and also has an inverse for any $n \in \mathbb{Z}$.

So if $(G, *)$ is a group, equations of the from $a * x = b$ for given $a, b \in G$ can be solved by multiplying a^{-1} on the left.

$$\begin{aligned} a^{-1} * (a * x) &= a^{-1} * b \\ (a^{-1} * a) * b &= a^{-1} * b \\ e * b &= a^{-1} * b \\ x &= a^{-1} * b. \end{aligned}$$

Note that all three properties of the group were used!

Example.

(1) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are all groups.

(2) $(\mathbb{N}, +), (\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot)$ are not groups, since they don't have an inverse for 0.

(3) $(\mathbb{Q}^\times, \cdot), (\mathbb{R}^\times, \cdot), (\mathbb{C}^\times, \cdot)$ are groups.

(4) The roots of unity with multiplication form a group.

Definition. (Commutative Group) A group G is **commutative/abelian** if

$$a * b = b * a \text{ for all } a, b \in G.$$

Proposition. (Basic properties of groups) Let G be a group.

(1) G has a unique identity.

(2) For $a \in G$, its inverse a^{-1} is unique.

(3) Left and right cancellation laws hold.

Remark. $(G, *)$ is a group $\iff$ $*$ is associative, has left identity, has left inverse.

Proof. ($\Longleftarrow$) Let e be a left identity of G. For any $a \in G$, let a' be a left inverse of a. Then, $a' * a * e = e * e = e = a' * a = a' * e * a$. Let a'' be a left inverse of a', then multiplying a'' on the left gives

$$a'' * a' * a * e = a'' * a' * e * a \implies a * e = e * a = a,$$

so $a * e = a$, proving that e is also a right identity.[2]

Let a' be a left inverse of a, and let a'' be a left inverse of a'. Then $a'' * a' * a * a' = e * a * a' = a * a'$, also $a'' * a' * a * a' = a'' * e * a' = a'' * a' = e$. Therefore $a * a' = e$, proving that a' is also a right inverse.[3]

Remark. For finite groups, the elements in a single row or column should be unique. For example, if some two elements $a * x$, $a * y$ in the same row (but different column) are the same, we can use the left cancellation law to show that $x = y$. This is a contradiction.

So, let $G = \{e, a\}$ be a group with identity e. Then its operation table is determined uniquely, as the following.

$*$	e	a
e	e	a
a	a	e

As for $G = \{e, a, b\}$, it is also unique.

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

[2] Alternatively, $ae = eae = (a''a')a(a'a) = a''ea'a = ea = a$.
[3] Alternatively, $aa' = (a''a')aa' = a''(a'a)a' = a''ea' = e$.

March 20th, 2023

Definition. (Equivalence Relation) A relation $\mathcal{R}$ on S is a **equivalence relation** if it satisfies the following.

(1) (Reflexive) $x\mathcal{R}x$. $(x \in S)$

(2) (Symmetric) If $x\mathcal{R}y$, then $y\mathcal{R}x$. $(x, y \in S)$

(3) (Transitive) If $x\mathcal{R}y$ and $y\mathcal{R}z$, then $x\mathcal{R}z$. $(x, y, z \in S)$

Example.

(1) Relation '=' on $\mathbb{Q} = \left\{\frac{y}{x} : x \in \mathbb{Z}^\times, y \in \mathbb{Z}\right\}$. Defined as $\frac{y}{x} = \frac{y'}{x'} \iff xy' = yx'$. The second equality is equality in $\mathbb{Z}$. We are defining '=' in $\mathbb{Q}$ using '=' in $\mathbb{Z}$.

(2) Relation '$>$' on $\mathbb{Z}$ is not symmetric, so it is not an equivalence relation.

Theorem. Equivalence relation $\sim$ on a set S yields a partition of S.

Example. Let $S = \mathbb{Z}$, $x \sim y \iff x \equiv y \pmod 5$. Then

$$\mathbb{Z} = \overline{0} \sqcup \overline{1} \sqcup \overline{2} \sqcup \overline{3} \sqcup \overline{4},$$

where $\overline{x} = \{y \in \mathbb{Z} : x \sim y\}$.

Section 5. Subgroups

Definition. (Subgroup) Let $(G, *)$ be a group, $H \subset G$. H is a **subgroup** of G if $(H, * \,|_{H\times H})$ is also a group. We write $H \leq G$.

Example.

(1) $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.

(2) (Trivial Subgroup) $\{e\} \leq G$.

(3) (Improper Subgroup) $G \leq G$.

(4) $\{e\} \leq \mathbb{Z}_2 \leq \mathbb{Z}_4$.

(5) $V_4 \not\cong \mathbb{Z}_4$ (different subgroup lattices).

(6) $\mathbf{SL}_n(\mathbb{R}) \leq \mathbf{GL}_n(\mathbb{R})$.

The following is a method to check that H is a subgrouop of G.

Theorem. Let G be a group and $H \subseteq G$. Then $H \leq G$ if and only if

(1) H is closed under the binary operation $*$ of G.

(2) Identity $e \in H$.

(3) For all $x \in H$, there exists an inverse $x^{-1} \in H$.

How can we find non-trivial subgroups? We include an element and generate elements, since the binary operations are always closed.

Theorem. Let G be a group, and let $a \in G$. Then

$$\{a^n : n \in \mathbb{Z}\} \leq G.$$

Proof. Let $H = \{a^n : n \in \mathbb{Z}\}$. Then for $a^n, a^m \in H$ $(n, m \in \mathbb{Z})$, $a^n a^m = a^{n+m} \in H$ (closed), $e = a^0 \in H$ (has an identity), $(a^n)^{-1} = a^{-n} \in H$ (has an inverse). So $H \leq G$.

Remark. Let $H = \{a^n : n \in \mathbb{Z}\}$.

(1) H is the smallest subgroup of G containing a.

(2) Any subgroup of G containing a has H as a subgroup.

(3) H is commutative.

Definition. (Cyclic) Let G be a group and let $H = \{a^n : n \in \mathbb{Z}\} \leq G$ for $a \in G$.

(1) H is called the **cyclic subgroup** generated by a, and we write $H = \langle a \rangle$.

(2) If there exists $x \in G$ such that $G = \langle x \rangle$, then G is called a **cylic group**.

Example. $U_n = \{\xi \in \mathbb{C} : \xi^n = 1\} = \langle \xi \rangle$, is a cyclic group where $\xi = e^{\frac{2\pi i}{n}}$. If we visualize this on the complex plane, the element ξ generates the whole group, in a cycle, hence the name cyclic group.

March 22nd, 2023

Section 6. Cyclic Groups

Theorem. Every cyclic group is commutative.

Always consider $U_n \simeq (\mathbb{Z}_n, +_n)$ as an example, when dealing with cyclic groups.

Theorem. A subgroup of a cyclic group is also cyclic.

Proof. Let $G = \langle g \rangle$ be a cyclic group, and let $H \leq G$. Choose the smallest positive $r \in \mathbb{N}$ such that $g^r \in H$. We show that $H = \langle g^r \rangle$. It is clear that $\langle g^r \rangle \leq H$, since H is a subgroup.

Suppose that there exists $s \in \mathbb{Z}$ such that $g^s \in H$, but $g^s \notin \langle g^r \rangle$. Then there exists unique quotient and remainder $q \in \mathbb{Z}, t \in \{1, \cdots, r-1\}$ such that $s = rq + t$. Then $g^s, g^{rq} \in H$, so $g^s(g^{rq})^{-1} = g^t \in H$, contradicting the minimality of r. Thus $H \leq \langle g^r \rangle$ and $H = \langle g^r \rangle$.

Example. $(\mathbb{Z}, +) = \langle 1 \rangle$. So any subgroup of $(\mathbb{Z}, +)$ should be $\langle n \rangle = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Definition. Let $S \subset G$. Then $\langle S \rangle$ is the smallest subgroup of G generated by S.

If $H = \langle a, b \rangle \leq \mathbb{Z}$, we can rewrite $H = \langle d \rangle$ for some $d \in \mathbb{Z}$. We know that $d = \gcd(a, b)$.

Definition. (Greatest Common Divisor) Let $r, s \in \mathbb{N}$. The **greatest common divisor** of r, s is the generator d which generates $\langle r, s \rangle \leq \mathbb{Z}$. We write $d = \gcd(a, b)$ and if $\gcd(r, s) = 1$, we say that r, s are **relatively prime**.

Remark. $\gcd(r, s) = 1 \iff mr + ns = 1$ for some $m, n \in \mathbb{Z}$.

We want to classify all cyclic groups!

Theorem. (Classification of Cyclic Groups) Suppose that $G = \langle g \rangle$ is cyclic.

(1) $|G| = \infty \iff G \simeq \mathbb{Z}$.

(2) $|G| = n \iff G \simeq \mathbb{Z}_n$.

Proof.
(1) Consider the map $\varphi : G \to \mathbb{Z}$, defined as $\varphi(g) = 1$. We first check that φ is well-defined. This is clear, since $|G| = \infty$, so $n \neq m \in \mathbb{Z} \iff g^n \neq g^m$. Otherwise, $|G|$ would be finite. This also implies that φ is bijective. Also φ is a homomorphism, since $\varphi(g^n g^m) = n + m = \varphi(g^n) + \varphi(g^m)$. φ is an isomorphism and $G \simeq \mathbb{Z}$.

(2) Consider the map $\varphi_n : G \to \mathbb{Z}_n$, defined as $\varphi_n(g) = 1$. We can check that φ_n is a well-defined isomorphism.

Theorem. Let $G = \langle a \rangle$ be a cyclic group of order n.

(1) Let $b = a^s \in G$. Then $|\langle b \rangle| = \dfrac{n}{\gcd(n, s)}$.

(2) $\langle a^s \rangle = \langle a^t \rangle \iff \gcd(n, s) = \gcd(n, t)$.

Proof. (1) We want to find the smallest positive integer m such that $b^m = e$. ($a^{ms} = e$, so $n \mid ms$) Take $d = \gcd(n, s)$, then $\gcd\left(\frac{n}{d}, \frac{s}{d}\right) = 1$. Since $\frac{n}{d} \mid \frac{s}{d} \cdot m$, then $\frac{n}{d} \mid m$. Hence the smallest positive integer m is $\frac{n}{d}$.

(2) Directly follows from (1). May have to prove that $\langle a^s \rangle = \langle a^t \rangle$.

Corollary. If $G = \langle a \rangle$ with order n, other generators of G are the elements of the form a^r where $\gcd(r, n) = 1$.

Part II

Permutations, Cosets and Direct Products

March 27th, 2023

Section 8. Groups of Permutations

Definition. (Permutation) A **permutation** on a set A is a bijective function $\varphi : A \to A$.

Remark. Let S_A be the set of permutations on A. Then $f \circ g \in S_A$ for all $f, g \in S$, $\circ$ has associativity, and $id \in S_A$, $f^{-1} \in S_A$ for all $f \in S$. Therefore $(S, \circ)$ is a group.

We study the case when A is a finite set, i.e, $A = \{1, 2, \ldots, n\}$.

Definition. (Symmetric Group S_n) Let $A = \{1, 2, \ldots, n\}$. Let S_n be the set of all permutations on A. Then $(S_n, \circ)$ is called the **symmetric group on n letters**.

Let B be a set with n elements. We denote S_B be the set of all permutations on B. With the composition operation $\circ$, we see that $S_B \simeq S_n$ as groups.

Example.

(1) $S_2 = \{e, \tau\}$ where $\tau = (1, 2)$.

(2) On S_3, there are 6 permutations.

$$S_3 = \{e, \mu_1, \mu_2, \mu_3, \rho_1, \rho_2\}$$

where μ_i swaps other two elements other than i, and $\rho_1 = (1, 2, 3), \rho_2 = (1, 3, 2)$.

(3) Also we can see that S_3 is the group of symmetries on an equilateral triangle. Each ρ_i represents a rotation, and each μ_i represents a reflection.

Remark. S_3 is not commutative. Check that $\rho_1 \circ \mu_1 = \mu_3$, but $\mu_1 \circ \rho_1 = \mu_2$. In fact, S_3 is the non-commutative group having the smallest order.

A natural question arises here: *Can we get S_n from the symmetries of a regular n-gon?*

Example. We try this for S_4, but this doesn't work. Symmetries of a square consists of 4 rotations and 4 reflections, which is a total of 8 elements, but $|S_4| = 4! = 24$.

Definition. (Dihedral Group D_n) The group of symmetries of a regular n-gon is called the **n-th dihedral group** D_n.

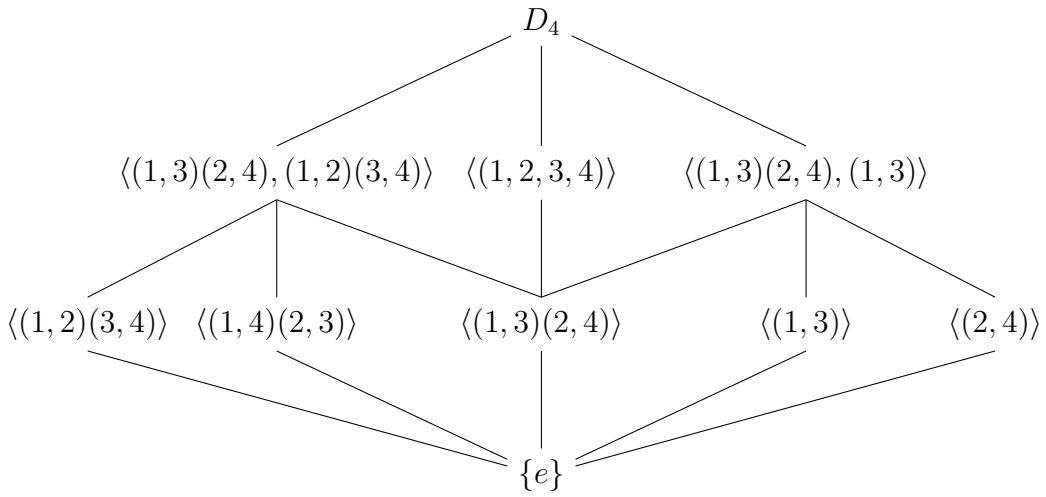
Remark.

(1) $D_3 \simeq S_3$, $D_4 < S_4$, D_4 is not commutative, so S_4 is not commutative.

(2) $|D_n| = 2n$.

(3) D_4 is generated by 2 elements. $D_4 = \langle \rho, \mu \rangle$, where ρ is a rotation by 90 degrees, and μ is some reflection.

(4) Subgroup lattice of D_4.



Lemma. For a group homomorphism $\varphi : G \to H$, $\operatorname{im} \varphi \leq H$. Additionally if φ is injective, $G \simeq \operatorname{im} \varphi \leq H$.

Proof. $\operatorname{im} \varphi$ is closed under the binary operation on H, since for any $a, b \in G$, $\varphi(a)\varphi(b) = \varphi(ab)$, and $ab \in G$, so $\varphi(a)\varphi(b) \in H$. $\varphi(e)$ is the identity, and $\varphi(a)^{-1} = \varphi(a^{-1})$. So $\operatorname{im} \varphi \leq H$. If φ is injective, restricting the range of φ to $\operatorname{im} \varphi$ gives an isomorphism, so $G \simeq \operatorname{im} \varphi$.

Why do we study symmetric groups? It is because of the following theorem. It states that all groups are isomorphic to some permutation group.

Theorem. (Cayley) Every group is isomorphic to some subgroup of S_n.

Proof. Consider $\varphi : G \to S_G$ such that $\varphi(g) = \lambda_g$, where $\lambda_g(x) = gx$ for $x \in G$. (left multiplication by g) We check that $\lambda_g \in S_G$, since groups have the cancellation law. Now check that φ is a monomorphism, then $G \simeq \operatorname{im} \varphi \leq S_G$.

Section 9. Orbits, Cycles and the Alternating Groups

Definition. Equivalence relation $\sim_\sigma$ on A with respect to $\sigma \in S_A$ is defined as

$$\text{For } a, b \in A,\ a \sim_\sigma b \iff \exists\, n \in \mathbb{Z} \text{ such that } a = \sigma^n(b).$$

Remark. Check that $\sim$ is indeed an equivalence relation.

Definition. (Orbit) Equivalence classes in A induced from the relation $\sim_\sigma$ are called the **orbits of** σ.

Example. Consider $\sigma = (1,3,6)(2,5,7,4)(8)$. Then $\{1,3,6\}, \{2,4,5,7\}, \{8\}$ are orbits.

If we represent orbits in circles, σ can be represented as 2 circles. $\tau = (1,2,3,4)$ would be represented as a circle, and $\tau' = (1,2,3)(4)$ would be represented as a circle.

Definition. (Cycles)

(1) A permutation $\sigma \in S_n$ is called a **cycle** if σ has at most 1 orbit with more than 1 element.

(2) The **length** of a cycle σ is the number of elements in its largest orbit.

τ is a cycle of length 4, τ' is a cycle of length 3, but σ is not a cycle.

Question. *For any $\sigma \in S_n$, can σ be represented as a composition of cycles?*

Theorem. Every permutation of a finite set is a product of disjoint cycles.

Proof. Take any $\sigma \in S_n$. Then the equivalence relation $\sim_\sigma$ induces a partition on $\{1, 2, \ldots, n\}$ as $\bigsqcup_{i=1}^{k} B_i$. Then $\sigma\,|_{B_i}\colon B_i \to B_i$ is a well-defined permutation. Now define

$$\mu_i(x) = \begin{cases} \sigma(x) & (x \in B_i), \\ x & (x \notin B_i). \end{cases}$$

Then μ_i is a cycle of B_i, and $\sigma = \mu_1 \circ \mu_2 \circ \cdots \circ \mu_k$.

Definition. (Transposition) A cycle of length 2 is called a **transposition**.

Remark. $(1,2,3) = (1,3)(1,2)$, $(a_1, a_2, \ldots, a_n) = (a_1, a_n)(a_1, a_{n-1}) \cdots (a_1, a_2)$.

Corollary. Any permutation is a product of transpositions, since disjoint cycles can be decomposed into a product of transpositions by the above remark.

Note that this representation is not unique. Since $\tau^2 = id$ for any transposition τ, we can always multiply two same transpositions at the end.

Theorem. No permutation in S_n can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

Proof.
(Step 1) Take $\sigma \in S_n$, transposition $\tau \in S_n$. Then for σ and $\tau\sigma$, their number of orbits differ by 1.

- Case 1. $\tau = (i, j)$ where i, j are not in the same orbit.
  Let $\sigma = (b, j, \dots)(a, i, \dots)(\dots)$. Then $\tau\sigma = (b, i, \dots, a, j, \dots)(\dots)$. So the number of orbits differ by 1.

- Case 2. $\tau = (i, j)$ where i, j are in the same orbit.
  Left as exercise.

(Step 2) Suppose we could write $\sigma = \tau_1\tau_2\cdots\tau_t = \tau_1'\tau_2'\cdots\tau_s'$ where τ_i, τ_j' are transpositions. Then the number of orbits of σ, t and s have the same parity. This follows directly from Step 1.

So this definition is well-defined!

Definition. A permutation $\sigma \in S_n$ is called

(1) **even** if σ is a product of even number of transpositions.

(2) **odd** if σ is a product of odd number of transpositions.

Definition. (Alternating Group A_n) We define the **alternating group** A_n as

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

Theorem.

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}.$$

Proof. Consider a map $\lambda_\tau : A_n \to S_n \setminus A_n$ defined as $\lambda_\tau(\sigma) = \tau \circ \sigma$ where τ is any transposition. Then λ_τ is a bijection.

April 3rd, 2023

Section 10. Cosets and the Theorem of Lagrange

Example. Motivation.

(1) $A_n \leq S_n$. We call $S_n \setminus A_n$ a coset of A_n.

(2) $3\mathbb{Z} \leq \mathbb{Z}$. We call $3\mathbb{Z}$, $3\mathbb{Z}+1$, $3\mathbb{Z}+2$ are cosets of $3\mathbb{Z}$.

We saw that A_n and $S_n \setminus A_n$ have the same number of elements. This was done by constructing a bijection between two sets. But we know that a bijection between $3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2$ exist. We guess that the number of elements would be the same for each coset.

So if G is a finite group and $H \leq G$, we conjecture that we can partition G by cosets of H, and each cosets have the same number of elements. So $|H| \mid |G|$.

Definition. Let G be a group, $H \leq G$. Define a relation $\sim_L$ on G as

$$a \sim_L b \iff a^{-1}b \in H.$$

Remark. We can also define $\sim_R$ on G as $a \sim_R b \iff ba^{-1} \in H$.

Theorem. $\sim_L$ is an equivalence relation.

Proof.

- $\forall a \in G$, $a^{-1}a = e \in H$. $a \sim_L a$.
- $\forall a, b \in G$, if $a^{-1}b \in H \implies (a^{-1}b)^{-1} = b^{-1}a \in H$. $b \sim_L a$.
- $\forall a, b, c \in G$, if $a^{-1}b, b^{-1}c \in H \implies (a^{-1}b)(b^{-1}c) = a^{-1}c \in H$. $a \sim_L c$.

Definition. (Coset) Let G, H be groups and $H \leq G$. For $a \in G$, we define

(1) The **left coset** of H as $aH = \{ah : h \in H\}$.

(2) The **right coset** of H as $Ha = \{ha : h \in H\}$.

We see that $a \neq b$ does not imply $aH \neq bH$. If $a, b \in H$, then $aH = bH = H$. So when would we get the same coset?

Remark. $aH = bH \iff H = a^{-1}bH \iff a \sim_L b$.

Example.

(1) For a transposition $\tau \in S_n$, τA_n is a coset of A_n with odd permutations. So it is different from A_n. So for any odd permutation $\sigma \in S_n$, $\sigma A_n = \tau A_n$, and $\sigma \sim_L \tau$.

(2) $3\mathbb{Z} \leq \mathbb{Z}$. $3\mathbb{Z}$, $3\mathbb{Z}+1$, $3\mathbb{Z}+2$ are cosets. Since $\mathbb{Z}$ is commutative, the left and right cosets are equal to each other.

Remark. If G is commutative and $H \leq G$, $aH = Ha$ for $a \in G$.

Check for non-commutative groups that left and rights cosets need not be equal!

Theorem. (Lagrange) Let G be a finite group with $H \leq G$. Then $|H| \mid |G|$.

Proof. If we construct a bijection between any two left cosets, $|H|$ would be $|G|$ divided by the number of left cosets. This would imply $|H| \mid |G|$.

Recall that left cosets are defined as the equivalence classes with respect to the relation $\sim_L$. So G is a disjoint union of cosets, $G = \bigsqcup aH$. Therefore, $|G| = (\text{number of left cosets}) \cdot |H|$.

Lemma. $|aH| = |bH|$ for $a \in G$, $H \leq G$.

Proof. $\varphi : aH \to bH$ is a bijection. Check by yourself!

Corollary. The number of left cosets and the number of right cosets are equal.

Corollary. Every group of prime order is cyclic.

Proof. Let $|G| = p$, where p is prime. Take $a \in G$ which is not the identity. Then the cyclic subgroup $\langle a \rangle \leq G$ must have order 1 or p. But a must have order p because it is not the identity. So $|\langle a \rangle| = p$, which implies that $G = \langle a \rangle$.

This is a very important result related to the classification of finite (simple) groups. We have seen all groups of order 2, 3, 4. But for larger orders, we can't enumerate them all. With this result, we directly know that for groups with prime order p, the group is isomorphic to $\mathbb{Z}_p$.

This is also a direct result of Lagrange's theorem, since $\langle a \rangle \leq G$.

Theorem. The order of an element in a finite group divides the order of the group. In other words, $|\langle a \rangle| \mid |G|$, for $a \in G$.

Definition. (Index) Let G be a group, (not necessarily finite) and $H \leq G$. We define the **index**

of H in G as

$$(G : H) = \text{number of left cosets of } H = \text{number of right cosets of } H.$$

If $|G| < \infty$, $(G : H) = |G| \,/\, |H|$.

Theorem. For a group G, suppose that $K \leq H \leq G$. If $(G : H)$, $(H : K)$ are finite,

$$(G : K) = (G : H)\,(H : K)\,.$$

Proof. Write $G = \bigsqcup_{i=1}^{n} a_i H$, $H = \bigsqcup_{j=1}^{m} b_j K$, and show that $G = \bigsqcup_{i,j} a_i b_j K$. Check by yourself!

Section 11. Direct Products, Finitely Generated Abelian Groups

Definition. (Cartesian Product) For sets $S_1, \ldots, S_n$, define

$$\prod_{i=1}^{n} S_i = S_1 \times S_2 \times \cdots \times S_n = \{(a_1, \ldots, a_n) : a_i \in S_i\}.$$

What if S_i already have a group structure?

Definition. (Direct Product) Let $G_1, \ldots, G_n$ be groups. Define a binary operation $\cdot$ as

$$(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n).$$

Then the **direct product** $\prod_{i=1}^{n} G_i$ is a group with this binary operation.

Notation. We also write the direct sum as $\bigoplus_{i=1}^{n} G_i$ for additive groups.

Example. Compare the Klein 4-group V_4 with $\mathbb{Z}_2 \times \mathbb{Z}_2$. They have the exact same structure! $V_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. From this example, we found out that order 4 group is either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Now we know all groups of order up to 5. How about order 6? We know S_3 and $\mathbb{Z}_6$.

Example. Consider $\mathbb{Z}_2 \times \mathbb{Z}_3$. We can check that $(1,1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ has order 6, so $\langle (1,1) \rangle = \mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$.

Why was it that $\mathbb{Z}_4 \neq \mathbb{Z}_2 \times \mathbb{Z}_2$, but $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$?

Theorem. $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$.

Proof.
($\Longleftarrow$) We need to find a generator of $\mathbb{Z}_m \times \mathbb{Z}_n$ with order mn. Take $a = (1,1) \in \mathbb{Z}_m \times \mathbb{Z}_n$. The order of this element should be divisible by m, n. So mn is the smallest positive integer, and $|\langle (1,1) \rangle| = mn$.

($\Longrightarrow$) Suppose that $d = \gcd(a, b) > 1$. Then for all $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, $\frac{mn}{d}(a, b) = (0, 0)$. So (a, b) cannot generate the entire group (which has mn elements). Therefore $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic.

April 10th, 2023

Corollary. $\prod_{i=1}^{n} \mathbb{Z}_{m_i} = \mathbb{Z}_{m_1} \times \cdots \mathbb{Z}_{m_n} \simeq \mathbb{Z}_{m_1 m_2 \cdots m_n} \iff \gcd(m_i, m_j) = 1$ for all $i \neq j$.

Example. Let $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ where p_i are distinct primes, $r_i \in \mathbb{N}$. Then

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$$

since $p_i^{r_i}$ are pairwise coprime.

Definition. (Least Common Multiple) Let $r_1, r_2, \ldots, r_m \in \mathbb{N}$. The **least common multiple** l of $r_1, r_2, \ldots, r_m$ is defined as the positive l such that

$$\langle l \rangle = \langle r_1 \rangle \cap \langle r_2 \rangle \cap \cdots \cap \langle r_m \rangle$$

in $\mathbb{Z}$. We write $l = \operatorname{lcm}(r_1, r_2, \ldots, r_n)$.

Theorem. Let $(a_1, \ldots, a_n) \in \prod_{i=1}^{n} G_i$, where each a_i has finite order r_i. Then

$$|(a_1, \ldots, a_n)| = \operatorname{lcm}(r_1, \ldots, r_n).$$

Proof. Homework! □

Example. $(8, 4, 10) \in \mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$. Then $r_1 = 3, r_2 = 15, r_3 = 12$. We want to find the smallest positive N such that $N(8, 4, 10) = (0, 0, 0)$. Then $3, 15, 12 \mid N$, so $N = \operatorname{lcm}(3, 5, 12) = 60$.

Structure of Finitely Generated Abelian Groups

A group is cyclic if it can be generated by a single element. Consider the Klein 4-group $V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$. This group has no element of order 4, so it is not cyclic. But we see that $V_4 = \langle (1,0), (0,1) \rangle$, so V_4 is generated by 2 elements. We extend this definition.

Definition. (Finitely Generated) A group G is **finitely generated** if there exists a finite subset $S \subset G$ such that $G = \langle S \rangle$.

Remark. If G is finite, $G = \langle G \rangle$ so it is finitely generated. But the converse is not true, since $\mathbb{Z}$ is infinite but $\mathbb{Z} = \langle 1 \rangle$.

We started learning from the simplest groups. They were generated by a single element and we classified them. We also learned about permutation groups and Cayley's theorem. Next, we classify a large family of groups. They are finitely generated abelian groups.

Theorem. (Fundamental Theorem of Finitely Generated Abelian Groups) Let G be a finitely generated abelian group. Then

$$G \simeq \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}} \times \overbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}^{\text{finite}}$$

where p_i are primes (not necessarily distinct), $r_i \in \mathbb{N}$, and this representation is unique up to order of products.

We only know cyclic groups, since they were the only groups that we classified completely. We studied permutation groups, but we saw that they are complex! So we don't know them very well, which leaves us to try a lot of things with cyclic groups. So we construct new groups from cyclic groups using direct products. Then we get this result that finitely generated abelian groups are actually a product of cyclic groups!

Remark. $\mathbb{Z}_4 \not\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. If these two groups were isomorphic, then it contradicts the uniqueness of product representation. Similarly, $\mathbb{Z}_9 \not\simeq \mathbb{Z}_3 \times \mathbb{Z}_3$ and $\mathbb{Z}_9 \times \mathbb{Z}_3 \not\simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

This is a typical exercise after learning this theorem.

Example. Classify all abelian groups of order 360.

Proof. This group is finitely generated. We know that $360 = 2^3 \times 3^2 \times 5$.

$$\begin{array}{cc} \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 & \mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 & \mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 & \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \end{array}$$

So these are all possible cases. □

Definition. (Decomposable) A group G is **decomposable** if $G \simeq H \times K$ for $H, K \leq G$.

This implies two things: that we can understand G by studying H, K, and that it is important to study indecomposable groups.

Theorem. A finite indecomposable abelian group is a cyclic group of order p^r where p is prime and $r \in \mathbb{N}$.

Theorem. Let G be a finite abelian group. If $m \mid |G|$, then there exists a subgroup of G with order m.

Proof. Let $G \simeq \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$. We use the fact that $\mathbb{Z}_{p_i^{s_i}} \leq \mathbb{Z}_{p_i^{r_i}}$ if $s_i \leq r_i$. Since $m \mid |G|$, we can write $m = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$ for some $s_i \leq r_i$. Take $H_i \leq \mathbb{Z}_{p_i^{r_i}}$ such that $|H_i| = p_i^{s_i}$. Then $H_1 \times H_2 \times \cdots H_k \leq G$, and it has order m. □

Recall that from Lagrange's theorem, for finite group G, if $H \leq G$, $|H| \mid |G|$. We could ask if the converse is true. *Is there a subgroup of order m that divides $|G|$?* This is not true in general, but if G is abelian this is true.

Theorem. Let m be a square-free integer.[1] Then an abelian group of order m is cyclic.

Proof. Let $m = p_1 \cdots p_k$ where p_i are distinct primes. Using the fundamental theorem, an abelian group of order m can be written as $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_k}$, which is isomorphic to $\mathbb{Z}_m$. □

[1] $\nexists p$ prime such that $p^2 \mid m$.

Part III

Homomorphisms and Factor Groups

Section 13. Homomorphisms

We already learned about homomorphisms.

Recall. Let G, G' be groups. A map $\varphi : G \to G'$ such that

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2), \quad \forall g_1, g_2 \in G$$

is called a **group homomorphism**. If φ is a bijection, φ is a **group isomorphism**.

Definition. Let $\varphi : G \to G'$ be a group homomorphism.

(1) (Kernel) The **kernel** of φ is

$$\ker \varphi = \{x \in G : \varphi(x) = e'\} = \varphi^{-1}(\{e'\}),$$

where e' is the identity of G'.

(2) (Image) The **image** of φ is

$$\operatorname{im} \varphi = \varphi(G) = \{\varphi(x) : x \in G\}.$$

April 12th, 2023

Theorem. Let $\varphi : G \to G'$ be a group homomorphism, $H = \ker \varphi$. For $a \in G$,

$$\varphi^{-1}(\varphi(a)) = aH = Ha.$$

Proof. ($\subset$) Take $g \in \varphi^{-1}(\varphi(a))$. Then $\varphi(g) = \varphi(a)$, and $e' = \varphi(e) = \varphi(ag^{-1})$, so $ag^{-1} \in \ker \varphi$. $ag^{-1} = h$ for some $h \in H$, and $g = h^{-1}a \in Ha$. Similarly $g \in aH$.

($\supset$) Let $g = ha \in Ha$ for some $h \in H$. Then $\varphi(g) = \varphi(ha) = \varphi(a)$, so $g \in \varphi^{-1}(\varphi(a))$. For $g \in aH$, it can be shown similarly. □

Corollary. φ is a monomorphism if and only if $\ker \varphi = \{e\}$.

Proof. ($\Longrightarrow$) Trivial. ($\Longleftarrow$) For $a \in G$, $\varphi^{-1}(\varphi(a)) = a\{e\} = \{a\}$. φ is injective. □

Here is an alternative elementary proof.

Proof. ($\Longleftarrow$) If $\varphi(x) = \varphi(y)$, then $\varphi(xy^{-1}) = e$, $xy^{-1} \in \ker \varphi$. So $xy^{-1} = e$ and $x = y$. □

Definition. (Normal Subgroup) Let $H \leq G$. If $aH = Ha$ for any $a \in G$, then H is called a **normal subgroup** of G. We write $H \trianglelefteq G$.

Corollary. $\ker \varphi \trianglelefteq G$ for any group homomorphism φ, since the left and right cosets coincide.

For injectivity, we can show that $\ker \varphi = \{e\}$ instead. We are on our way to define factor groups.

Section 14. Factor Groups

If $H \leq G$, $\{aH : a \in G\}$ were left cosets. We want to give a group structure on the cosets. Not just any structure, but a structure that naturally arises from the structure of G. $(aH)(bH) = abH$ is a natural candidate, but we have a problem. *Is this operation well-defined?* If $aH = a'H$ and $bH = b'H$, is it true that $abH = a'b'H$? Sadly, this is not true in general. But it is true when $aH = Ha$.[1]

Definition. (Factor Group) If $H \leq G$, G/H is defined as

$$G/H = \{aH : a \in G\}.$$

If G/H has a group structure with the binary operation $(aH)(bH) = abH$, we call G/H a **factor group**.

[1] Not math: $(aH)(bH) = a(Hb)H = a(bH)H = abH$, so we want $bH = Hb$!

Example. $\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}\}$.

Theorem. Let $\varphi : G \to G'$ be a group homomorphism.

(1) $G/\ker\varphi$ is a factor group.

(2) (1st Isomorphism Theorem) $G/\ker\varphi \simeq \operatorname{im}\varphi$, with isomorphism $\mu(a\ker\varphi) = \varphi(a)$.

Proof.
(1) Well-definedness! If $a\ker\varphi = a'\ker\varphi$ and $b\ker\varphi = b'\ker\varphi$, then $\varphi(a) = \varphi(a')$ and $\varphi(b) = \varphi(b')$. Since φ is a homomorphism, $\varphi(ab) = \varphi(a'b')$. So $ab\ker\varphi = a'b'\ker\varphi$. Associativity directly follows, eH is the identity, $a^{-1}H = (aH)^{-1}$ can be checked.

(2) Well-definedness! If $a\ker\varphi = a'\ker\varphi$, then $\varphi(a) = \varphi(a')$, so $\mu(a\ker\varphi) = \mu(a'\ker\varphi)$. The fact that μ is an isomorphism can be checked easily. □

If we prove the well-definedness part, the rest is pretty automatic.

Recall. $N \trianglelefteq G \iff gN = Ng$ for all $g \in G \iff gNg^{-1} = N$ for all $g \in G$.

Theorem. For $H \leq G$, G/H is a factor group if and only if $H \trianglelefteq G$.

Proof. ($\Longleftarrow$) Trivial.
($\Longrightarrow$) Let $x \in aH$. Choose $x \in aH$, $a^{-1} \in a^{-1}H$. then $H = (aH)(a^{-1}H) = (xH)(a^{-1}H) = (xa^{-1})H$. So $xa^{-1} \in H$, showing that $x \in Ha$. Similarly, $Ha \subset aH$. $H \trianglelefteq G$. □

Definition. The G/H in the above theorem is called a **factor group** or a **quotient group**.

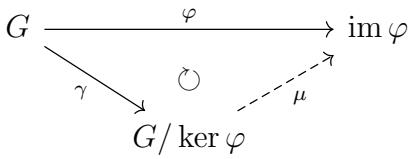
April 17th, 2023

This theorem implies that a normal subgroup is a kernel of some homomorphism.[2]

Theorem. (Fundamental Homomorphism Theorem) Let $\varphi : G \to G'$ be a group homomorphism. Then $\operatorname{im}\varphi$ is a group, and $\mu : G/\ker\varphi \to \operatorname{im}\varphi$ defined as

$$\mu(a\ker\varphi) = \varphi(a), \quad a \in G,$$

is an isomorphism.



Theorem. If $H \leq G$, The following are equivalent.

(1) $H \trianglelefteq G$.

(2) $gHg^{-1} = H$ for all $g \in G$.

(3) $ghg^{-1} \in H$ for all $g \in G$, $h \in H$.

(4) $gH = Hg$ for all $g \in H$.

Definition. (Automorphism)

(1) An isomorphism $\varphi : G \to G$ is called an **automorphism**.

(2) $i_g : G \to G$ defined as $i_g(x) = gxg^{-1}$ is called the **inner automorphism** by g.

(3) gxg^{-1} is called a **conjugation** of x by g.

(4) For $H \leq G$, $i_g(H) = gHg^{-1}$ is called the **conjugation subgroup** of H.

(5) If $i_g(H) = H$ then H is called **invariant**.

Remark. Normal subgroups of G are invariant under all inner automorphisms.

[2] Natural projection $\pi : G \to G/N$, $\ker\pi = N$.

Section 15. Factor Group Computations & Simple Groups

We want to see if some quotient group is a group we already know!

Example.

(1) $\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}$.

(2) $A_n \trianglelefteq S_n$, since $\tau A_n = A_n \tau$ for any transposition τ. (a permutation is either odd or even) Then $(S_n : A_n) = 2$, and since a group of order 2 is unique, we have $S_n/A_n \simeq \mathbb{Z}_2$.

Theorem. If $H \leq G$ with $(G : H) = 2$, $H \trianglelefteq G$ and $G/H \simeq \mathbb{Z}_2$.

Proof. Write $G = H \sqcup aH$ where $a \in G \setminus H$. Similarly, $G = H \sqcup Ha$. So $aH = Ha = G \setminus H$. Therefore $H \trianglelefteq G$, and G/H is a quotient group with order 2. Since $\mathbb{Z}_2$ is the only group of order 2, $G/H \simeq \mathbb{Z}_2$. □

Recall. (Lagrange) Let G be a finite group with $H \leq G$. Then $|H| \mid |G|$.

Proposition. The converse of Lagrange's Theorem does not hold.

Proof. Consider A_4. Suppose that there is a subgroup H of order 6. Then $A_4/H \simeq \mathbb{Z}_2$. Then for any $\sigma \in A_4$, $\sigma^2 \in H$. Since $(i,j,k)^2 = (i,k,j)$ and $(i,k,j)^2 = (i,j,k)$, every 3-cycle should be in H. There are 8 3-cycles in A_4, so $|H| \neq 6$. □

Theorem. For groups H, K, let $G = H \times K$. Let $\overline{H} = H \times \{e_K\} \leq G$. Then $\overline{H} \trianglelefteq G$ and $K \simeq G/\overline{H}$.

Proof.
(Method 1) For any $(h,k) \in G$, $(h,k)^{-1}(h', e_k)(h,k) \in \overline{H}$ for all $h, h' \in K$ and $k \in K$. Then the map $\varphi : K \to G/\overline{H}$ defined as $\varphi(k) = (\overline{e_H}, k)$ is an isomorphism. □

(Method 2) Consider $\varphi : G \to K$ defined as $\varphi(h,k) = k$, and show that φ is an epimorphism with $\ker \varphi = \overline{H}$. The result directly follows from the first isomorphism theorem. □

Example. $(\mathbb{Z}_4 \times \mathbb{Z}_6) \,/\, \langle (0,2) \rangle$. We see that $\langle (0,2) \rangle = \{(0,0), (0,2), (0,4)\}$, so the order of the quotient group should be $24/3 = 8$. By the fundamental theorem of FGAG, this group should be isomorphic to one of $\mathbb{Z}_8$ or $\mathbb{Z}_4 \times \mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

- $\mathbb{Z}_4 \times \mathbb{Z}_6$ does not have an element of order greater than 8, so G/H doesn't either. $G/H \not\simeq \mathbb{Z}_8$.
- For $(1,0) \in \mathbb{Z}_4 \times \mathbb{Z}_6$, $2(1,0) = (2,0) \notin \langle (0,2) \rangle$. So $(1,0)$ has order greader than 2 in G/H.

So $G/H \not\simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Therefore $G/H \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$.

There are lots of exercises like this. We see another example with infinite order. We cannot enumerate all cases like above in this example.

Example. $(\mathbb{Z} \times \mathbb{Z}) / \langle (1,1) \rangle$. Consider $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined as $\varphi(a,b) = a - b$. Next, show that φ is an epimorphism and that $\ker \varphi = \langle (1,1) \rangle$. Then $(\mathbb{Z} \times \mathbb{Z}) / \langle (1,1) \rangle \simeq \mathbb{Z}$ by the first isomorphism theorem.

Why do we study quotient groups? First, we get new kinds of groups. Second, for finitely generated abelian groups, we like to write them in their decomposed form since we know cyclic groups *very* well. So we can handle them. But for non-commutative groups, we cannot use this approach. So we want 'simple' groups, that will be a building block for larger groups.

Definition. (Simple Group) A group is **simple** if it does not have a nontrivial proper normal subgroup. i.e. only normal subgroups are $\{e\}$ and itself.

We state this theorem and use it without proof. The insolvability of the quintic comes from this statement.

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

If simple groups are the building blocks, there should be a way to derive simple groups from any group.

Definition. (Maximal Normal Subgroup) M is a **maximal normal subgroup** of G if for any *proper* $N \lhd G$, $N \subseteq M$.

Theorem. M is a maximal normal subgroup of G if and only if G/M is simple.

April 19th, 2023

Proposition. Let $\varphi : G \to G'$ be a group homomorphism.

(1) $N \trianglelefteq G \implies \varphi(N) \trianglelefteq \varphi(G)$.

(2) $N' \trianglelefteq \varphi(G) \implies \varphi^{-1}(N') \trianglelefteq G$.

Proof. For any $\varphi(g) \in \varphi(G)$, $\varphi(g)\varphi(n)\varphi(g)^{-1} = \varphi(gng^{-1}) \in \varphi(N)$. □

Remark. $\varphi(N) \trianglelefteq G'$ is not true! For $K \trianglelefteq H \trianglelefteq G'$, $K \trianglelefteq H$ does not imply $K \trianglelefteq G'$. (not transitive) Think about the definition of normal subgroups. $K \trianglelefteq H \iff aK = Ka$ for all $a \in H$, but as for $K \trianglelefteq G'$, $aK = Ka$ for all $a \in G'$. So if we extend to a larger group, it may not be a normal subgroup.

Theorem. M is a maximal normal subgroup of G if and only if G/M is simple.

Proof. The projection $\varphi : G \to G/M$, $\varphi(g) = gM$ is a group homomorphism.

($\implies$) Suppose that M is a maximal normal subgroup and G/M is not simple. Then there exists proper $\overline{P} \lhd G/M = \varphi(G)$ which is not trivial. Then $\varphi^{-1}(\overline{P}) \lhd G$ is a normal subgroup which strictly contains M.

($\impliedby$) Suppose that G/M is simple and M is not maximal. Then there exists $P \lhd G$ such that $M \subsetneq P$. Then $\varphi(P) \lhd G/M$ is a nontrivial proper normal subgroup. □

Center & Commutator Subgroup

Definition. (Center) The center of a group G is defined as

$$Z(G) = \{z \in G : gz = zg,\ \forall g \in G\}.$$

Remark. $Z(G) \trianglelefteq G$.

Definition. (Commutator Subgroup)

(1) For $a, b \in G$, $aba^{-1}b^{-1}$ is called the **commutator** of G.

(2) $C = \langle aba^{-1}b^{-1} : a, b \in G \rangle \leq G$ is called the **commutator subgroup**.

The following theorem is the reason we use commutator subgroups. Think about the meaning. Center of a group is used to get a commutative subgroup of G. Commutator subgroup is used to quotient out the non-commutative elements, to get a commutative group.

Theorem. Let C be the commutator subgroup of G.

(1) $C \trianglelefteq G$.

(2) If $N \trianglelefteq G$, G/N is commutative if and only if $C \subset N$.

Proof. (1) Let $g \in G$, $aba^{-1}b^{-1} \in C$. We want to show that $g^{-1}aba^{-1}b^{-1}g \in C$.

$$g^{-1}aba^{-1}b^{-1}g = g^{-1}aba^{-1}(gb^{-1}bg^{-1})b^{-1}g = (g^{-1}a)b(g^{-1}a)^{-1}b^{-1}(bg^{-1}b^{-1}g) \in C.$$

(2) Left as exercise. □

Section 16. Group Action on a Set

This is a very important section! Groups appear on many branches of mathematics.

Definition. (G-set) Let G be a group and X be a set. A **group action** of G on X is a map $G \times X \to X$ such that

(1) If e is the identity of G, $ex = x$ for all $x \in X$.

(2) $(g_1g_2)x = g_1(g_2x)$ for all $g_1, g_2 \in G$ and $x \in X$.

The set X is called a **G-set**.

Example.

(1) $X = G$, consider a map $G \times X \to X$, where $(g_1, g_2) \mapsto g_1g_2$. X is a G-set.

(2) Let $G = S_n$, $X = \{1, 2, \ldots, n\}$. Consider a map $G \times X \to X$ defined as $(\sigma, x) \mapsto \sigma(x)$. X is a S_n-set.

Theorem. Let X be a G-set. For each $g \in G$, the function $\sigma_g : X \to X$ defined by $\sigma_g(x) = gx$ is a permutation of X. Also, the map $\varphi : G \to S_X$ defined by $\varphi(g) = \sigma_g$ is a homomorphism with the property $\varphi(g)(x) = gx$.

Definition. Let X be a G-set.

(1) G acts **faithfully** on X if $\{a \in G : ax = x,\ \forall x \in X\} = \{e\}$.

(2) G acts **transitively** on X if for any $x_1, x_2 \in X$, $\exists\, g \in G$ such that $gx_1 = x_2$.

April 24, 2023

We can consider G/N-action on X. If G is not transitive, we can make it transitive by quotienting it out by N. (Why?)

Example. Think about the definitions...

(1) Consider the numbered square and D_4. Then D_4 acts on X transitively.

(2) Refer to Example 16.8. There doesn't exist an element of D_4 such that $m_1 \mapsto d_1$. This action is not transitive.

Isotropy Subgroups

Definition. Given a G-set X, fix $g \in G$, $x \in X$.

(1) $X_g = \{x \in X : gx = x\} \subset X$. (Fixed points)

(2) (Isotropy Subgroup) $G_x = \{g \in G : gx = x\} \subset G$.

$X_g \subset X$ always, but is $G_x \leq G$?

Theorem. Let X be a G-set. For $x \in X$, $G_x \leq G$.

Proof. For $g_1, g_2 \in G_x$, $(g_1g_2)x = g_1(g_2x) = g_1x = x$, so $g_1g_2 \in G_x$. Also $ex = x$ so $e \in G_x$. If $g \in G_x$, $g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = x$, so $g^{-1} \in G_x$. □

Can we partition or classify elements of X with respect to the actions of G?

Theorem. Given a G-set X, for $x_1, x_2 \in X$, define

$$x_1 \sim x_2 \iff \exists\, g \in G \text{ such that } gx_1 = x_2.$$

Then $\sim$ is an equivalence relation.

Proof. Left as exercise. □

So X has a partition induced by the action of G. Each equivalence class is an orbit.

Definition. (Orbit) Given a G-set X, the **orbit** of x under G as

$$Gx = \{gx : g \in G\}.$$

Remark. Do not get confused! $Gx \subset X$, $G_x \leq G$.

Theorem. (Orbit-Stabilizer Theorem) Given a G-set X, let $x \in X$. Then $|Gx| = (G : G_x)$.

Proof. Let H be the left cosets of G_x, define $\varphi : Gx \to H$ by $\varphi(gx) = gG_x$. We show that φ is a bijection. Well-definedness! Does $g_1x = g_2x$ imply $g_1G_x = g_2G_x$? The reverse direction shows that φ is injective. Then surjectivity is trivial if we have well-definedness. Left as exercise. □

By Lagrange's Theorem, $|Gx| = |G| / |G_x|$, so we have $|G| = |Gx| \cdot |G_x|$.

Section 17. Applications of G-sets to Counting

Theorem. (Burnside's Formula) Let $|G| < \infty$, X be a finite G-set. Let r be the number of orbits. Then

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

Proof. By double counting, note that

$$\sum_{g \in G} |X_g| = \sum_{x \in X} |G_x| = |\{(g, x) \in G \times X : gx = x\}|\,.$$

By the orbit-stabilizer theorem,

$$\sum_{g \in G} |X_g| = \sum_{x \in X} \frac{|G|}{|Gx|} = |G| \sum_{\text{orbit } \mathcal{O}} \sum_{x \in \mathcal{O}} \frac{1}{|Gx|} = r\,|G|\,.$$

Here, $\sum_{x \in \mathcal{O}} \frac{1}{|Gx|} = \sum_{x \in \mathcal{O}} \frac{1}{|\mathcal{O}|} = 1$, so the last equality holds. □

Example. We have a cube with 6 faces, where we want to mark the faces with 6 distinct marks. Then how many are distinguishable?

Proof. If a cube can be rotated to give the same markings, they are not distinguishable. Let X be the set of all distinct markings. Then $|X| = 6! = 720$. (We treat all 6 faces as distinct faces) Let G be the group of rotations of the cube, then $|G| = 6 \times 4 = 24$. Then the number of orbits of X under G is equal to the number of distinguishable cubes. By Burnside's formula, $r = \frac{1}{|G|} \sum_{g \in G} |X_g|$. We can check that $X_e = X$, and if $g \neq e$, $|X_g| = 0$. So $r = \frac{720}{24} = 30$. □

Part VII

Advanced Group Theory

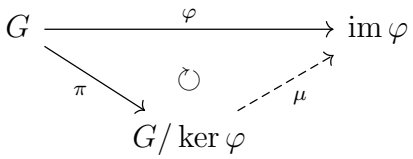
April 26th, 2023

Section 34. Isomorphism Theorems

Theorem. (First Isomorphism Theorem) Let $\varphi : G \to G'$ be a group homomorphism. Then $\mu : G/\ker\varphi \to \operatorname{im}\varphi$ defined as

$$\mu(x \ker\varphi) = \varphi(x), \quad (x \in G)$$

is an isomorphism, and $G/\ker\varphi \simeq \operatorname{im}\varphi$.



Lemma. Let $N \trianglelefteq G$ and $\gamma : G \to G/N$ be a canonical homomorphism. Then

$$\varphi : \{M \trianglelefteq G : N \leq M\} \to \{K \trianglelefteq G/N\}$$

defined as $\varphi(M) = \gamma(M)$ is a bijection.

Proof. Since γ is a epimorphism, if $M \trianglelefteq G$, then $\varphi(M) = \gamma(M) \trianglelefteq \gamma(G) = G/N$. We next show that φ is a bijection. $\varphi(L) = \varphi(M)$, then $\gamma(L) = \gamma(M)$ so $L = M$. This works because $N \leq M$ and $\gamma^{-1}(\gamma(M)) = M$. Also, for $K \trianglelefteq G/N$, $\varphi(\gamma^{-1}(K)) = K$. □

Recall. We proved a part of this when we proved that if M is a maximal normal subgroup, then G/M is simple.

Notation. For $H, N \leq G$, define $H \vee N = \langle H, N \rangle$.

Lemma.

(1) If $N \trianglelefteq G$ and $H \leq G$, $HN = NH \leq G$. i.e. $H \vee N = HN = NH$.

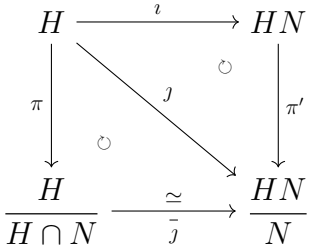
(2) If $N \trianglelefteq G$ and $H \trianglelefteq G$, then $H \vee N = HN \trianglelefteq G$.

Proof.
(1) Let $h_1 n_1, h_2 n_2 \in HN$ for $h_i \in H, n_i \in N$. Since $N \trianglelefteq G$, $\exists\, n_3 \in N$ such that $h_1 n_1 h_2 n_2 = h_1 h_2 n_3 n_2$, which is an element of HN. Check that $e \in HN$, $(hn)^{-1} \in HN$.

(2) For $g \in G$, we show that $ghng^{-1} \in HN$ for $h \in H$, $n \in N$. Since both subgroups are normal, there exists $h' \in H$, $n' \in N$ such that $hng^{-1} = g^{-1}h'n'$. Then $ghng^{-1} = (gg^{-1})h'n' \in HN$. □

Theorem. (Second Isomorphism Theorem) If $H \leq G$ and $N \trianglelefteq G$,

$$\frac{HN}{N} \simeq \frac{H}{H \cap N}.$$



Proof. We first have to check that $N \trianglelefteq HN$ and $H \cap N \trianglelefteq H$. (Check!)

Consider $\gamma : G \to G/N$. It is clear that γ is surjective.

- $\gamma\,|_H \colon H \to \gamma(H)$
- $\gamma\,|_{HN} \colon HN \to \gamma(HN)$. Actually, $\gamma(HN) = \gamma(H)$.

By the first isomorphism theorem,

$$\frac{H}{\ker \gamma\,|_H} \simeq \gamma(H) \simeq \frac{HN}{\ker \gamma\,|_{HN}}.$$

Now we check that $\ker \gamma\,|_H = H \cap N$ and $\ker \gamma\,|_{HN} = N$. This is trivial. □

Example. Let $G = \mathbb{Z}_{24}$, $H = \langle 4 \rangle$, $N = \langle 6 \rangle$. Then

$$HN = \{n4 + m6 : n, m \in \mathbb{Z}\} = \langle 2 \rangle, \quad H \cap N = \langle 4 \rangle \cap \langle 6 \rangle = \langle 12 \rangle.$$

We see that $HN/N \simeq H/H \cap N \simeq \mathbb{Z}_3$.

Theorem. (Third Isomorphism Theorem) If $H, K \trianglelefteq G$ and $K \leq H$,[1] then

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

Proof. We first have to check that $K \trianglelefteq H$ and $H/K \trianglelefteq G/K$. (Check the first)

Let $\overline{g} \in G/K$, $\overline{h} \in H/K$. We show that $\overline{g} \cdot \overline{h} \cdot \overline{g^{-1}} \in H/K$, this is trivial. Define

$$\varphi : G \xrightarrow{\psi_1} G/K \xrightarrow{\psi_2} \frac{G/K}{H/K}.$$

We check that φ is a well-defined group homomorphism, and that φ is surjective, and $\ker \varphi = H$. Then the result directly follows from the first isomorphism theorem. □

Example. Let $G = \mathbb{Z}$, $H = 2\mathbb{Z}$, $K = 6\mathbb{Z}$. $G/K \simeq \mathbb{Z}_2$, $G/K \simeq \mathbb{Z}_6$, $H/K \simeq \mathbb{Z}_3$. Then $\mathbb{Z}_2 \simeq \mathbb{Z}_6/\mathbb{Z}_3$ (abuse of notation) by the third isomorphism theorem.

Section 35. Series of Groups

Given a group G, we want to decompose G with simpler groups, $G \rightsquigarrow G_1 * G_2 * \cdots * G_k$. We consider a series of normal subgroups,

$$\cdots \trianglelefteq N_3 \trianglelefteq N_2 \trianglelefteq N_1 \trianglelefteq G.$$

Then we can consider a sort of a situation like

$$G = G/N_1 * N_1/N_2 * N_2/N_3 * \cdots$$

and if each normal subgroup is maximal, then each term is simple! This leads us to the Jordan-Hölder theorem. We will use the second/third isomorphism theorems.

[1] This implies that $K \trianglelefteq H$.

May 1st, 2023

Definition. Given a finite sequence of subgroups

$$\{e\} = H_0 < H_1 < \cdots < H_k = G,$$

(1) (Subnormal Series) If $H_i \lhd H_{i+1}$ for $i = 0, \ldots, k-1$, it is called a **subnormal series**.

(2) (Normal Series) If $H_i \lhd G$ for $i = 0, \ldots, k-1$, it is called a **normal series**.

Note that the *finite* condition is important!

Remark. Since $H_i \lhd G \implies H_i \lhd H_{i+1}$, a normal series is a subnormal series.

We will focus on subnormal series.

Example. Let $G = \mathbb{Z}$. Since G is abelian, all subgroups are normal, so

$$\{0\} = H_0 < 12\mathbb{Z} < 6\mathbb{Z} < 3\mathbb{Z} < \mathbb{Z} = G$$

is a subnormal series. Also,

$$\{0\} = H_0 < 18\mathbb{Z} < 9\mathbb{Z} < 3\mathbb{Z} < \mathbb{Z} = G.$$

We see that subnormal series are not unique, and note that we can find an infinite series of subgroups of $\mathbb{Z}$. But actually we want uniqueness, since we want to find the building blocks of a group. How can we obtain a *unique* subnormal series, up to isomorphism?

Definition. Subnormal (normal) series $\{H_i\}_{i\in I}$, $\{K_j\}_{j\in J}$ of G are **isomorphic** if there exists a bijection between

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

such that the corresponding quotient groups are isomorphic.

Example. Consider the following subnormal series,

$$\{H_i\} : \{0\} < \{0, 2, 4, 6\} < \mathbb{Z}_8, \quad \{K_j\} : \{0\} < \{0, 2\} < \mathbb{Z}_8.$$

We know that $H_2/H_1 \simeq \mathbb{Z}_2$, $H_1/H_0 \simeq \mathbb{Z}_4$, and $K_2/K_1 \simeq \mathbb{Z}_4$, $K_1/K_0 \simeq \mathbb{Z}_2$. So we will map H_2/H_1 to K_1/K_0, and H_1/H_0 to K_2/K_1. So these two series are isomorphic. The building blocks of $\mathbb{Z}_8$ obtained from the two series are equivalent!

Definition. (Refinement) For two subnormal (normal) series $\{H_i\}$ and $\{K_j\}$ of G, $\{K_j\}$ is a **refinement** of $\{H_i\}$ if $\{H_i\} \subset \{K_j\}$.

Example. Given a subnormal series $\{H_i\}$: $\{0\} < \langle 8\rangle < \langle 2\rangle < \mathbb{Z}_{24}$, we can insert $\langle 4\rangle$ to get a subnormal series

$$\{K_j\} : \{0\} < \langle 8\rangle < \langle \mathbf{4}\rangle < \langle 2\rangle < \mathbb{Z}_{24}.$$

Now, each K_{j+1}/K_j has no nontrivial proper subgroups.

We are one step closer to getting uniqueness.

Theorem. (Schrier) Any two subnormal (normal) series of G have isomorphic refinements.

Remark. This theorem does not state that for any two pairs of subnormal series, their isomorphic refinements are isomorphic. i.e. if $\{H_i\}, \{K_i\}, \{L_i\}, \{M_i\}$ are subnormal series of G, the isomorphic refinements obtained from $\{H_i\}, \{K_i\}$ and $\{L_i\}, \{M_i\}$ need not be isomorphic. So we don't have the exact uniqueness. As an example, consider the following series

$$\{0\} < 36\mathbb{Z} < 12\mathbb{Z} < 3\mathbb{Z} < \mathbb{Z}, \quad \{0\} < 72\mathbb{Z} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}.$$

We can obtain many isomoprhic refinements by appending some $n\mathbb{Z}$ to the end of the series. So the isomorphic refinements can change, depending on the last element of the series.

Example. Consider these subnormal series,

$$\{0\} < \langle 8\rangle < \langle 2\rangle < \mathbb{Z}_{24}, \quad \{0\} < \langle 12\rangle < \langle 6\rangle < \mathbb{Z}_{24}.$$

We can obtain a refinement by

$$\{0\} < \langle 8\rangle < \langle \mathbf{4}\rangle < \langle 2\rangle < \mathbb{Z}_{24}, \quad \{0\} < \langle 12\rangle < \langle 6\rangle < \langle \mathbf{3}\rangle < \mathbb{Z}_{24}.$$

These two series are isomorphic.

Definition. Let $\{H_i\}$ be a subnormal (normal) series of G. If H_{i+1}/H_i is simple for any i, $\{H_i\}$ is called a **composition (principal) series**.

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

Remark. We assumed something that wasn't an assumption in the Schrier theorem. Does G really have a composition series? Consider the series $\{0\} < n\mathbb{Z} < 6\mathbb{Z} < 3\mathbb{Z} < \mathbb{Z}$. This cannot be a composition series, since any multiple m of n, the quotient group $n\mathbb{Z}/\{0\} \simeq n\mathbb{Z}$ has a subgroup $m\mathbb{Z}$. So this series is infinite, thus $\mathbb{Z}$ has no composition series. In Jordan-Hölder theorem, we are assuming that G has a composition series, which gets rid of groups that don't have a composition series.

Proof. Composition series cannot have any further refinements. By Schrier theorem. □

Proof. (of Schrier, Idea sketch) Consider two subnormal series

$$\{0\} = H_0 \leq H_1 \leq \cdots \leq H_i \leq H_{i+1} \leq \cdots H_k = G,$$

$$\{0\} = K_0 \leq K_1 \leq \cdots \leq K_j \leq K_{j+1} \leq \cdots \leq K_l = G.$$

Then in between $H_i \leq H_{i+1}$, write

$$H_i(K_0 \cap H_{i+1}) \leq H_i(K_1 \cap H_{i+1}) \leq \cdots \leq H_i(K_l \cap H_{i+1}).$$

In between $K_j \leq K_{j+1}$, write

$$K_j(H_0 \cap K_{j+1}) \leq K_j(H_1 \cap K_{j+1}) \leq \cdots \leq K_j(H_k \cap K_{j+1}).$$

Our claim is that if we obtain a refienment by applying the above to all pairs, we can get an isomorphic subnormal series.

Claim. $H_i(K_{j+1} \cap H_{i+1})/H_i(K_j \cap H_{i+1}) \simeq K_j(H_{i+1} \cap K_{j+1})/K_j(H_i \cap K_{j+1})$.

Proof. By the following lemma. □

Lemma. (Zassenhaus) Suppose that $H^* \trianglelefteq H$, $K^* \trianglelefteq K$, $H, K \leq G$. Then the following hold.

(1) $H^*(H \cap K^*) \trianglelefteq H^*(H \cap K)$.

(2) $K^*(H^* \cap K) \trianglelefteq K^*(H \cap K)$.

(3) $H^*(H \cap K)/H^*(H \cap K^*) \simeq K^*(H \cap K)/K^*(H^* \cap K) \simeq H \cap K/(H^* \cap K)(H \cap K^*)$.

Proof. Consider $\varphi : H^*(H \cap K) \to H \cap K/(H^* \cap K)(H \cap K^*)$, that maps $\varphi(hx) = \overline{x}$. ($h \in H^*$, $x \in H \cap K$) We need to check the following.

- $H^*(H \cap K)$ is a group.
- $H \cap K/(H^* \cap K)(H \cap K^*)$ is a quotient group. ($H^* \cap K, H \cap K^* \trianglelefteq H \cap K$)
- φ is a well-defined epimorphism.
- $\ker \varphi = H^*(H \cap K^*)$.

Then the result follows from the first isomorphism theorem. □

Part IV

Rings and Fields

May 3rd, 2023

Section 18. Rings and Fields

Definition. (Ring) $(R, +, \cdot)$ is a **ring** if it satisfies the following properties.

(1) $(R, +)$ is an abelian group.[1]

(2) $\cdot$ is associative.

(3) (Distributive) $a(b+c) = ab + ac$, $(a+b)c = ac + bc$.[2]

Remark. In our textbook, ring R may not have a multiplicative identity. Some authors require that a ring should have a multiplicative identity. We also denote the multiplicative identity as 1. The inverse of a is a^{-1} as usual.

Example. Examples of rings.

(1) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$.

(2) $\mathcal{M}_{n\times n}(R)$, the set of matrices whose entries are in the ring R.

(3) $n\mathbb{Z} = \langle n \rangle$ is a ring without 1, for $n \neq 0, \pm 1$. Note that $\mathbb{Z}$ and $n\mathbb{Z}$ are isomorphic as groups, but it is not isomorphic as rings.

(4) $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

[1] We will write 0 as the additive identity, $-a$ as the additive inverse of a.
[2] The two binary operations are *compatible*.

(5) (Direct Product of Rings) If $R_1, \ldots, R_n$ are rings, then $R_1 \times \cdots \times R_n$ is also a ring, where the multiplication is done componentwise.

Theorem. Let $a, b \in R$.

(1) $0 \cdot a = a \cdot 0 = 0$.

(2) $a(-b) = (-a)b = -ab$.

(3) $(-a)(-b) = ab$.

Proof. Exercise. □

Since homomorphisms and isomorphisms were defined on any binary structures, we can specialize the definition to ring homomorphisms and isomorphisms.

Definition. For rings R, R', $\varphi : R \to R'$ is a **ring homomorphism** if

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b), \quad \forall a, b \in R.$$

If φ is bijective, then φ is a **ring isomorphism**.

Example.

(1) $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ defined as $\varphi(n) = \overline{n}$ is a ring homomorphism.

(2) $\varphi : \mathbb{Z} \to 2\mathbb{Z}$ defined as $\varphi(n) = 2n$ is not a ring homomorphism. $\varphi(1) \neq \varphi(1)\varphi(1) = 4$.

Remark. Note that if the binary operation changes, φ may not be a homomorphism anymore. Homomorphisms were defined on the set *with the binary operation*, not on the set itself.

Proposition. For $r, s \in \mathbb{Z}$, if $\gcd(r, s) = 1$, $\mathbb{Z}_{rs} \simeq \mathbb{Z}_r \times \mathbb{Z}_s$ as rings.

Proof. We know already that these are isomorphic as groups. Check also for multiplication, with the isomorphism $\varphi : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$ defined as $\varphi(n \cdot 1) = n \cdot (1, 1)$. □

We cannot say much about multiplication on rings, since it only satisfies associativity. We want to consider some examples where the multiplication has more properties.

Definition. Let R be a ring.

(1) (Commutative Ring) R is a **commutative ring** if $ab = ba$ for all $a, b \in R$.

(2) (Ring with Unity) R is a **ring with unity** if R has a multiplicative identity $1 \in R$.

We kind of hope that $(R, \cdot)$ becomes a group. We have associativity and assume a lot that it has an identity. How about inverses? But since $0 \cdot a = 0$ for any $a \in R$, not all elements can have inverses.

Definition. Let R be a ring with unity.

(1) (Unit) If $u \in R$ has a multiplicative inverse $u^{-1} \in R$, u is called a **unit**.

(2) (Division Ring) R is a **division ring** if all non-zero elements have an inverse.

(3) (Field) A **field** is a commutative division ring.

Remark. For a field F, $(F \setminus \{0\}, \cdot)$ is a group.

Example. Examples of fields.

(1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

(2) $\mathbb{Z}_p$ is a field if p is prime.

Definition. Let R be a ring and F be a field.

(1) (Subring) If $S \subset R$ and S is a ring by the binary operations inherited from R, then S is called a **subring** of R and write $S \leq R$.

(2) (Subfield) If $K \subset F$ and K is a field by the binary operations inherited from F, then F is called a **subfield** of F and write $K \leq F$.

May 8th, 2023

Section 19. Integral Domains

Keep in mind $(\mathbb{Z}, +, \cdot)$ and $(\mathbb{R}[x], +, \cdot)$.

We considered linear equations of the form $ax = b$ where a, b are elements of a group G. Since we have associativity and inverses, we could solve the equation. But in a ring, we can't do the same thing. How would we solve $3n = 12$ in $\mathbb{Z}$? We know for sure that $n = 4$, but we don't have a proof yet. We will learn *cancellation*, then we will be able to write $3 \cdot n = 3 \cdot 4$ and cancel 3 to get $n = 4$.

Example. Solve $x^2 - 5x + 6 = 0$ in $\mathbb{Z}_{12}$.

Remark. If we were to solve this in $\mathbb{Z}$, we factor the equation and get $x = 2$ or $x = 3$. But in $\mathbb{Z}_{12}$, we have to solutions $x = 2, 3, 6, 11$. We see that $\mathbb{Z}$ and $\mathbb{Z}_{12}$ are different in some way.

Definition. (Zero Divisor) Let R be a ring. For $a \in R \setminus \{0\}$, if $\exists\, b \in R \setminus \{0\}$ such that $ab = 0$, then a is called a **zero divisor**.

Remark. We know that $\mathbb{Z}$ has no zero divisors. However in $\mathbb{Z}_{12}$, 3 and 4 are zero divisors.

Returning to the example $3n = 12$, rewrite using the distributive law to get $3(n-4) = 0$. Since $\mathbb{Z}$ has no zero divisors, $n - 4$ must be 0. We have $n = 4$. Zero divisors let us solve equations.

Theorem. m is a zero divisor of $\mathbb{Z}_n$ if and only if $\gcd(m, n) \neq 1$.

Proof. ($\Longleftarrow$) If $\gcd(m, n) = d > 1$, then $m \cdot \frac{n}{d} = \frac{m}{d} \cdot n = 0$ in $\mathbb{Z}_n$.

($\Longrightarrow$) If $\gcd(m, n) = 1$, then $mr = 0$ in $\mathbb{Z}_n$ if and only if $n \mid r$. So $r = 0$, contradiction. $\square$

Corollary. If p is prime, $\mathbb{Z}_p$ has no zero divisors.

Definition. (Cancellation Law) For a ring R, we say that **cancellation laws** hold in R if

$$[ab = ac \implies a = 0 \text{ or } b = c] \text{ or } [ac = bc \implies c = 0 \text{ or } a = b] \text{ for } a, b, c \in R.$$

Theorem. For a ring R, cancellation laws hold in R if and only if R has no zero divisors.

Proof. ($\Longleftarrow$) If there are no zero divisors, $ab = ac$ implies $a(b - c) = 0$, so $a = 0$ or $b = c$.

($\Longrightarrow$) Let $a, b \in R$ such that $ab = 0$. Then $ab = a0$, so $a = 0$ or $b = 0$ by cancellation law. $\square$

So this is how we can solve $3n = 12$ in $\mathbb{Z}$, which has no zero divisors.

Definition. (Integral Domain) If a commutative ring with unity has no zero divisors, it is called an **integral domain**.

Example.

(1) $\mathbb{Z}, \mathbb{Z}_p$ (p: prime) are integral domains.

(2) $\mathbb{Z}_n$ where n is not prime, is not an integral domain.

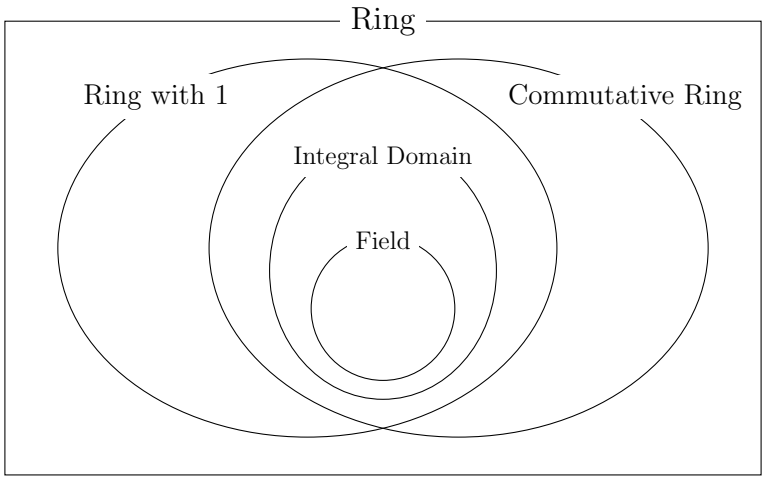
(3) For ring R, S, $R \times S$ is not an integral domain since $(r, 0)(s, 0) = (0, 0)$.

We compare integral domains with fields.

Theorem. If F is a field, then F is an integral domain.

Proof. Let $a, b \in F$ with $ab = 0$. If $a \neq 0$, multiply a^{-1} on the left to get $b = 0$. □

The following diagram shows the relations between ring structures.



Theorem. Every finite integral domain is a field.

Proof. Let $D = \{a_0, \ldots, a_n\}$ be an integral domain. For nonzero $a \in D$, consider the set $aD = \{aa_0, aa_1, \ldots, aa_n\}$. We show that $aD = D$. Since D is finite, it is enough to show that $aa_i \neq aa_j$ for $i \neq j$. This is clear since D is an integral domain. Since $1 \in aD$, $\exists\, a_i \in D$ such that $aa_i = 1$. So $\exists\, a^{-1} = a_i$, concluding that D is a field. □

Proof. (Another) Let $x \in D \setminus \{0\}$. Then consider $x, x^2, \ldots$. Due to finiteness, $x^n = x^m$ for two distinct $n, m \in \mathbb{N}$. Then $x^{n-m} = 1$ by cancellation. We conclude that x has an inverse. □

Corollary. If p is prime, $\mathbb{Z}_p$ is a field.

Characteristic of Ring

Definition. (Characteristic)

(1) Let R be a ring. If there exists $n \in \mathbb{N}$ such that $na = 0$ for all $a \in R$, then the least such integer n is called the **characteristic** of R and write $\operatorname{char} R = n$.

(2) If there does not exist such integer, we say that the characteristic of R is zero.

Theorem. Let R be a ring with unity, and let $n \in \mathbb{N}$. Then $\operatorname{char} R = n$ if and only if n is the smallest positive integer such that $n \cdot 1 = 0$.

Proof. ($\Longrightarrow$) Trivial.

($\Longleftarrow$) For all $a \in R$,

$$na = \overbrace{a + a + \cdots + a}^{n \text{ times}} = a(1 + 1 + \cdots + 1) = a(n \cdot 1) = a0 = 0.$$

So $\operatorname{char} R = n$, since n is the smallest positive integer. □

May 15th, 2023

Section 20. Fermat's and Euler's Theorems

Remark. If F is a field, then $(F^\times, \cdot)$ is a group.

Proof. $F^\times$ is closed under multiplication, is associative, has identity and has inverse. □

Theorem. (Fermat's Little Theorem) For $a \in \mathbb{Z}$ and prime p such that $p \nmid a$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. The statement can be rewritten as follows. For $a \neq 0$ in $\mathbb{Z}_p$, $a^{p-1} = 1$ in $\mathbb{Z}_p$. Since $\mathbb{Z}_p^\times$ is a group of order $p-1$, the order of a should divide $p-1$. Therefore, $a^{p-1} = 1$ in $\mathbb{Z}_p$. □

Corollary. For $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$ for any prime p.

Proof. If $p \nmid a$, the result directly follows from Fermat's little theorem. If $p \mid a$, then $a \equiv 0 \pmod{p}$, so $a^n \equiv a \equiv 0 \pmod{p}$. □

Example. $8^{103} \equiv (8^{12})^8 \cdot 8^7 \equiv 1 \cdot 8^7 \equiv (8^2)^3 \cdot 8 \equiv (-1)^3 \cdot 8 \equiv 5 \pmod{13}$.

Example. Show that $15 \mid (n^{33} - n)$ for any integer n.

Proof. We show that 3, 5 both divide the given expression. Use Fermat's little theorem. □

We have Euler's generalization.

Theorem. Let $G_n = \{a \in \mathbb{Z}_n \setminus \{0\} : a \text{ is not a zero divisor}\}$. Then $(G_n, \cdot)$ is a group.

Proof. G_n is closed under multiplication. For $a, b \in G_n$, suppose that $(ab)c = 0$ for some $c \in \mathbb{Z}_n$. Then $a(bc) = 0$, so $bc = 0$ and $c = 0$. So ab is not a zero divisor. Also $ab \neq 0$, since a, b are not zero divisors. Thus $ab \in G_n$.

Next, multiplication is associative and we know that $1 \in G_n$. Lastly, $a \in G_n$ has an inverse. Let $G_n = \{a_0 = 1, a_1, \ldots, a_k\}$. Then $aG_n = \{a, aa_1, \ldots, aa_k\}$. But the elements of aG_n are distinct, since if $aa_i = aa_j$ for some different i, j, then $a(a_i - a_j) = 0$. a is not a zero divisor so $a_i = a_j$, which contradicts that a_i are distinct. So there exists $b \in G_n$ such that $ab = 1$. Then $b = a^{-1} \in G_n$. G_n is a multiplicative group. □

Definition. (Euler Phi Function) For $n \in \mathbb{N}$, define $\varphi(n)$ as the number of positive integers $k \leq n$ such that $\gcd(n, k) = 1$.

Example. $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(12) = 4$.

Theorem. (Euler) Let $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof. Let G_n be the set of nonzero elements which are not zero divisors in $\mathbb{Z}_n$. Then $|G_n| = \varphi(n)$. Take $a \in G_n$, then $a^{|G_n|} = a^{\varphi(n)} = 1$ in G_n. The result directly follows since if $\gcd(a, n) = 1$ then a is not a zero divisor in $\mathbb{Z}_n$. (Theorem 19.3) □

Example. $7^4 \equiv 1 \pmod{12}$, since $7 \in G_{12}$ ($\gcd(7, 12) = 1$) and $\varphi(12) = 4$.

We solve linear congruences with the above results.

Theorem. Let $m \in \mathbb{N}$, $a \in \mathbb{Z}_m$ such that $\gcd(a, m) = 1$. Then for all $b \in \mathbb{Z}_m$, there exists a unique solution to $ax = b$ in $\mathbb{Z}_m$.

Proof. Since $\gcd(a, m) = 1$, $a \in G_m$, and $\exists\, a^{-1} \in G_n \subset \mathbb{Z}_m$. Therefore $x = a^{-1}b$ is the unique solution to $ax = b$. If x_1, x_2 were solutions, multiplying a^{-1} on both sides of $ax_1 = ax_2$ would give $x_1 = x_2$. □

Corollary. Let $a, m \in \mathbb{Z}$, $\gcd(a, m) = 1$. For all $b \in \mathbb{Z}$, there exists a solution in $\mathbb{Z}$ to $ax \equiv b \pmod{m}$. All solutions are in one residue class modulo m.

Theorem. Let $m \in \mathbb{N}$, $a \in \mathbb{Z}_m$ and let $\gcd(a, m) = d$. The equation $ax = b$ has a solution in $\mathbb{Z}_m$ if and only if $d \mid b$. If $d \mid b$, then there are exactly d solutions in $\mathbb{Z}_m$.

Proof. Homework. □

Corollary. Let $a, m \in \mathbb{Z}$, and let $\gcd(a, m) = d$. Then $ax \equiv b \pmod{m}$ has a solution if and only if $d \mid b$. If $d \mid b$, every solution is in d distinct residue classes.

Example. Solve $12x \equiv 27 \pmod{18}$.

Proof. $\gcd(12, 18) = 6$, but $6 \nmid 27$, so this equation has no solution. □

Example. Solve $15x \equiv 27 \pmod{18}$.

Proof. $\gcd(15, 18) = 3$ and $3 \mid 27$, so are 3 classes of solutions. By inspection $x = 3$ is a solution, and $15 \cdot 6 = 15 \cdot \frac{18}{3} = 5 \cdot 18 \equiv 0 \pmod{18}$, so $15x \equiv 15(x + 6) \pmod{18}$. Thus $x = 9, 15$ are also solutions. Thus $x \equiv 3, 9, 15 \pmod{18}$. □

May 17th, 2023

Section 21. The Field of Quotients of an Integral Domain

Motivation: we have an integral domain $\mathbb{Z}$, we want to create a field $\mathbb{Q}$. We embed $\mathbb{Z}$ into $\mathbb{Q}$ to use useful properties of fields.[3]

Define $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0\right\}$ and $\frac{a}{b} = \frac{c}{d} \iff ad = bc$. Each $\frac{a}{b}$ is an equivalence class. The operations are defined as

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad + bc}{bd}\right],\ \left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right].$$

Given an integral domain D, we want to construct $D \hookrightarrow F$ (field). As a set, let

$$S = \{(a, b) : a, b \in D,\ b \neq 0\}.$$

Definition. Let $(a, b), (c, d) \in S$. $(a, b) \sim (c, d) \iff ad = bc$.

Check that $\sim$ is an equivalence relation. Note that we need the cancellation law of D.

Definition. Let $F = \{[(a, b)] : (a, b) \in S\}$. Addition and multiplication are defined as

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)], \quad [(a, b)] \cdot [(c, d)] = [(ac, bd)].$$

Lemma. Addition and multiplication on F are well-defined.

Proof. We show that if $(a, b) \sim (a', b')$, $(c, d) \sim (c', d')$, then $[(a, b)] * [(c, d)] = [(a', b')] * [(c', d')]$ for both multiplication and addition. Trivial. □

Lemma. The following holds.

(1) Addition on F is associative, has identity and inverse.

(2) Multiplication on F is associative, has identity, and has inverse for $a \in F \setminus \{0\}$.

(3) Addition and multiplication on F are compatible.

(4) Multiplication and addition on F are commutative.

Proof. Check associativity. Additive identity is $[(0, 1)]$, $-[(a, b)] = [(-a, b)]$. Multiplicative identity is $[(1, 1)]$, $[(a, b)]^{-1} = [(b, a)]$, if the inverse exists. □

[3] A similar example is when we calculate eigenvalues in $\mathbb{C}$, instead of $\mathbb{R}$.

Lemma. Let $\iota : D \hookrightarrow F$ where $\iota(a) = [(a, 1)]$. Then ι is a monomorphism and $\iota(D) \simeq D$.

Proof. Left as exercise. □

Remark. $[(a, b)] = [(a, 1)] \cdot [(1, b)] = \iota(a)\iota(b)^{-1}$.

Is this the most natural construction?

Theorem. Let D be an integral domain. Then D can be embedded into a field F such that every element of F can be expressed as a quotient of two elements of D.

Definition. (Field of Quotients) Such F is called the **field of quotients** of D.

Remark. The first condition $D \hookrightarrow F$ tells us that F contains D. Every element of F should be expressible, so F shouldn't be too large. This construction also gives us uniqueness.

Let F be a field of quotients of D. Then $F = \left\{\frac{a}{b} : a, b \in D,\, b \neq 0\right\}$. We know that $\frac{a}{b} \cdot b = a$, $\frac{a}{b} = \frac{c}{d} \iff ad = bc$.

How should multiplication be defined? Suppose that $\frac{a}{b} \cdot \frac{c}{d} = x$. Multiplying bd on both sides gives $xbd = ac$, so $x = \frac{ac}{bd}$. This can be done similarly for addition, which implies that addition and multiplication on F has to be defined this way.

Theorem. Let F be a field of quotients of D, let L be any field such that $D \subset L$. Then there exists $\psi : F \to L$ such that $\psi(a) = a$ for $a \in D$ and $F \simeq \psi(F) \leq L$.

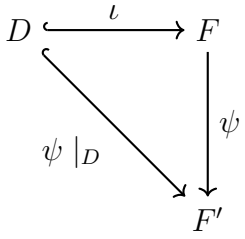
Proof. Define $\psi\left(\frac{a}{b}\right) = ab^{-1}$ for $a, b \in D$, $b \neq 0$. Check that ψ is well-defined, and that ψ is a monomorphism. □

Corollary.

(1) Any field containing D contains a field of quotients of D.

(2) Any two fields of quotients of D are isomorphic.

Proof. (2) Let F, F' be two fields of quotients of D.



Check that ψ is onto, $a \cdot_F b^{-1} \mapsto a \cdot_{F'} b^{-1}$. □

May 22nd, 2023

Section 24. Noncommutative Examples

Definition. (Endomorphism) An **endomorphism** is a homomorphism into itself. The set of endomorphisms of an abelian group A is denoted as $\mathrm{End}(A)$.

Example. Ring of endomorphisms.

(1) For $\varphi, \psi \in \mathrm{End}(A)$ and $a \in A$ define the binary operations

$$(\varphi + \psi)(a) = \varphi(a) + \psi(a), \quad (\varphi * \psi)(a) = (\varphi \circ \psi)(a).$$

Then $\mathrm{End}(A)$ is a noncommutative ring, since composition is not commutative.

(2) $A = F[x] = \left\{\sum_{n=0}^{k} a_n x^n : a_n \in F\right\}$, where $\mathrm{char}\, F = 0$. Take $X, Y \in \mathrm{End}(A)$ such that

$$X(f(x)) = xf(x), \quad Y(f(x)) = \frac{\partial}{\partial x} f(x).$$

Let $W = \langle X, Y \rangle$ be the subring of $\mathrm{End}(A)$ generated X, Y. W is called the *Weyl algebra*.

Proposition. The Weyl algebra W is not commutative.

Proof. For $f(x) \in F[x]$, we show that $(XY - YX)(f(x)) \neq 0$. By simple calculus,

$$YX(f(x)) = \frac{\partial}{\partial x}(xf(x)) = f(x) + x\frac{\partial}{\partial x} f(x) = f(x) + XY(f(x)).$$

Thus $YX - XY = 1$. □

Group Rings and Group Algebras

Let $G = \{g_i : i \in I\}$ be a group, and let R be a commutative ring with unity.

Proposition. $RG = \left\{\sum_{i \in I} a_i g_i : a_i \in R, g_i \in G\right\}$ is a ring, with the binary operations defined as

$$\sum a_i g_i + \sum b_i g_i = \sum (a_i + b_i) g_i, \quad \left(\sum a_i g_i\right)\left(\sum b_i g_i\right) = \sum_{k \in I} \sum_{g_i g_j = g_k} (a_i b_j) g_k.$$

If G is not commutative, $R[G]$ is not commutative.

Definition. RG is called the **group ring of G over R**, and if F is a field, FG is called the **group algebra of G over F**.

The Quaternions

$\mathbb{H} = (\mathbb{R}^4, +)$, denote an element by $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$. We define multiplication as

$$\mathbf{ij} = \mathbf{k}, \quad \mathbf{jk} = \mathbf{i}, \quad \mathbf{ki} = \mathbf{j}, \quad \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1.$$

$\mathbb{H}$ is noncommutative division ring with unity. (Not a field)

Section 22. Ring of Polynomials

Definition. (Ring of Polynomials) Let R be a ring. Then the **ring of polynomials over** R is defined as

$$R[x] = \left\{ \sum_{i=0}^{N} r_i x^i : r_i \in R \right\}.$$

Here, the x is called an **indeterminate**. Addition and multiplicaion is defined as

$$\sum a_i x^i + \sum b_i x^i = \sum (a_i + b_i) x^i, \quad \left(\sum a_i x^i \right) \left(\sum b_i x^i \right) = \sum_k \sum_{i+j=k} (a_i b_j) x^k.$$

Definition. (Degree) The **degree** of a polynomial $p(x) = \sum_{i=1}^{N} r_i x^i$ is the largest n such that $r_n \neq 0$, and we write $\deg p(x) = n$.[4]

Remark. If R is commutative, check that $R[x]$ is a commutative ring.

Example. Let p be prime. In $\mathbb{Z}_p$,

$$(x+1)^p = \sum_{i=0}^{p} \binom{p}{i} x^i = x^p + 1.$$

since p always divides $\binom{p}{i}$ for $i = 1, \ldots, p-1$. In general,

$$(ax+b)^p = a^p x^p + \sum_{i=1}^{p-1} a^i b^{p-i} \binom{p}{i} x^i + b^p = (ax)^p + b^p = ax^p + b,$$

since $a^p = a$, $b^p = b$ in $\mathbb{Z}_p$ by Fermat's little theorem.

Remark.

(1) For integral domain D, $D[x]$ is an integral domain.

(2) For field F, $F[x]$ is an integral domain.

[4]The degree of the zero polynomial is not defined. Some texts use $-\infty$.

(3) For integral domain D, $(D[x])[y] \simeq (D[y])[x]$ is also an integral domain. We can define $D[x, y]$ in this way, and inductively define $D[x_1, \ldots, x_n]$.

Notation. Let $F(x) = \left\{ \frac{g(x)}{f(x)} : f(x), g(x) \in F[x],\ f(x) \neq 0 \right\}$ be the field of quotients of $F[x]$.

Evaluation Homomorphism

Theorem. Let E be a field, and $F \leq E$. For $\alpha \in E$, the map $\varphi_\alpha : F[x] \to E$ defined as

$$\varphi_\alpha(f) = f(\alpha), \quad f \in F[x].$$

Then φ_α is a ring homomorphism.

Definition. (Evaluation Homomorphism) φ_α above is called the **evaluation homomorphism**.

Remark. We know that $f(x) = x^2 + 1 \in \mathbb{R}[x]$ has the solution $x = i$. We write this rigorously as: for the evaluation homomorphism $\varphi_i : R[x] \to \mathbb{C}$, $\varphi_i(f) = 0$.

Definition. (Zero) Let E be a field, and $F \leq E$. For $f \in F[x]$, if $\varphi_\alpha(f) = 0$ for $\alpha \in E$, then α is called a **zero** of f.

May 24th, 2023

Section 23. Factorization of Polynomials over a Field

Let F be a field.

Theorem. (Division Algorithm for $F[x]$) For $f(x), g(x) \in F[x]$, let

$$f(x) = a_n x^n + \cdots + a_0, \quad g(x) = b_m x^m + \cdots + b_0, \quad (a_n, b_m \neq 0, n, m \in \mathbb{N}).$$

There exists unique polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

where $\deg r(x) < m$ or $r(x) = 0$.

Proof. (Existence) Define a set

$$S = \{f(x) - s(x)g(x) : s(x) \in F[x]\} \subset F[x].$$

If $0 \in S$, then $\exists\, q(x) \in F[x]$ such that $f(x) = q(x)g(x) + 0$. So assume $0 \notin S$. Then there is a polynomial $r(x)$ with minimal degree in S. We need to show that $\deg r < \deg g$.

Suppose not, and denote $r(x) = c_l x^l + \cdots + c_0$ where $l = \deg r$. Then by calculation, degree of $r'(x) = r(x) - \frac{c_l}{b_m} x^{l-m} \cdot g(x)$ is less than $l = \deg r$. However, since $r'(x) \in S$, it contradicts that $r(x)$ has the minimal degree in S.

(Uniqueness) Suppose that for $q(x), q'(x), r(x), r'(x) \in F[x]$,

$$f(x) = q(x)g(x) + r(x) = q'(x)g(x) + r'(x),$$

with [$\deg r < \deg g$ or $r = 0$] and [$\deg r' < \deg g$ or $r' = 0$]. We have $g(x)(q(x) - q'(x)) = r'(x) - r(x)$. LHS is 0 or has degree at least $\deg g$, RHS is 0 or has degree less than $\deg g$. Since they are equal they are both 0, and we have $q(x) = q'(x)$ and $r(x) = r'(x)$. □

Remark. We needed that F is a field in c_l/b_m. If F is changed to D, we cannot use this proof.

Corollary. (Factor Theorem) $a \in F$ is a zero of $f(x) \in F[x]$ if and only if $(x - a) \mid f(x)$.

Proof. ($\Longleftarrow$) If $f(x) = (x - a)g(x)$ for some $g(x) \in F[x]$, $\varphi_a(f(x)) = 0 \cdot \varphi_a(g(x)) = 0$.

($\Longrightarrow$) By the division algorithm, $\exists\, q, r \in F[x]$ such that $f(x) = (x - a)g(x) + r(x)$ and $r(x) \in F$. By evaluation at a, $\varphi_a(f(x)) = \varphi_a((x - a)g(x)) + r$ implies that $r = 0$. □

Example. Let $f(x) = x^4 + 3x^3 + 2x + 4 \in \mathbb{Z}_5[x]$. $f(1) = 0$, so $f(x) = (x-1)(x^3 + 4x^2 + 4x + 1)$. Repeat the process to get $f(x) = (x-1)^3(x+1)$.

Corollary. Let $0 \neq f(x) \in F[x]$ with $\deg f = n$. Then $f(x)$ has at most n distinct zeros in F.

Proof. Suppose that $\{a_1, \ldots, a_m\}$ are distinct zeros of $f(x)$. By the factor theorem, $f(x)$ can be written as

$$f(x) = (x - a_1)(x - a_2) \ldots (x - a_m)g(x)$$

from some $g \in F[x]$. Then $n = \deg f \geq m$. □

Corollary. Let G be a finite subgroup of $(F^\times, \cdot)$. Then G is cyclic.

Proof. G has to be a finite abelian group. So by the fundamental theorem of finitely generated abelian groups,

$$G \simeq \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \mathbb{Z}_{p_k^{r_k}}.$$

Let $l = \operatorname{lcm}(p_1^{r_1}, p_2^{r_2}, \ldots, p_k^{r_k})$. Then for all $g \in G$, $g^l = 1$, so all $g \in G \subset F$ is a zero of $f(x) = x^l - 1 \in F[x]$. Let m be the number of distinct zeros of $f(x)$.

m should be at least $|G| = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$. But by the above corollary, $l \geq m$. Therefore $\operatorname{lcm}(p_1^{r_1}, p_2^{r_2}, \ldots, p_k^{r_k}) = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$. We conclude that p_i, p_j are pairwise relatively prime, and $G \simeq \mathbb{Z}_{p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}}$. □

Irreducible Polynomials

Definition. (Irreducible Polynomial) Let $f(x) \in F[x]$, which is not a constant.

(1) If there exists $g(x), h(x) \in F[x]$ with $\deg g, \deg h < \deg f$ such that $f(x) = g(x)h(x)$, then $f(x)$ is **reducible**.

(2) If f is not reducible, it is **irreducible**.

Example. $f(x) = x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, but reducible in $\mathbb{R}[x]$.

Theorem. If $f(x) \in F[x]$ is a reducible polynomial of degree 2 or 3, then $f(x)$ has a zero.

Proof. f is reducible, so it must have a factor of degree 1. $3 = 1 + 2$, $2 = 1 + 1$. □

If f is reducible in $\mathbb{Q}[x]$, then it is reducible in $\mathbb{Z}[x]$.

Theorem. Let $f(x) \in \mathbb{Z}[x]$. $f(x) = g(x)h(x)$ for $g(x), h(x) \in \mathbb{Q}[x]$ with $\deg g, \deg h < \deg f$ if and only if there exists $\widetilde{g}, \widetilde{h} \in \mathbb{Z}[x]$ such that $f(x) = \widetilde{g}(x)\widetilde{h}(x)$, $\deg \widetilde{g} = \deg g$ and $\deg \widetilde{h} = \deg h$.

Corollary. For $n \geq 1$, let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. If f has a zero in $\mathbb{Q}$, then f has a zero $m \in \mathbb{Z}$ such that $m \mid a_0$.

Proof. Let $f(x) = (ax + b)g(x)$ with $a \neq 0$. Then $f(x) = (\widetilde{a}x + \widetilde{b})\widetilde{g}(x) \in \mathbb{Z}[x]$. So comparing coefficients of x^n and x^0 will give $\widetilde{a} = \pm 1$, $\widetilde{b} \mid a_0$. Then $\pm\widetilde{b}$ is a zero of f. □

Example. Is $f(x) = x^4 - 2x^2 + 8x + 1 \in \mathbb{Q}[x]$ irreducible? If $f(x)$ had a linear factor, then $f(x)$ has a zero in $\mathbb{Z}$, and that zero should be a divisor of 1. $f(1), f(-1) \neq 0$, so this is impossible. Next, we need to show that there are no polynomials $g, h \in \mathbb{Z}[x]$ of degree 2, such that $f(x) = g(x)h(x)$. We do this by setting

$$f(x) = (x^2 + ax + 1)(x^2 + bx + 1) = (x^2 + cx - 1)(x^2 + dx - 1),$$

and showing that such $a, b, c, d \in \mathbb{Z}$ do not exist. Note that this is possible since we are in $\mathbb{Z}$. If we were in $\mathbb{Q}$, we would have many cases to consider.

May 29th, 2023

Note that we cannot use the division algorithm in $D[x]$.

Now, how do we check if a polynomial is irreducible?

Theorem. (Eisenstein Criterion) For $p \in \mathbb{Z}$ prime, and $n \geq 1$, let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

f is irreducible over $\mathbb{Q}$ if $a_n \not\equiv 0 \pmod{p}$, $a_i \equiv 0 \pmod{p}$ for $i < n$ and $a_0 \not\equiv 0 \pmod{p^2}$.

Proof. It is enough to show that f is irreducible over $\mathbb{Z}$. Suppose that $\exists\, g(x), h(x) \in \mathbb{Z}[x]$ such that $f(x) = g(x)h(x)$. Denote

$$g(x) = b_m x^m + \cdots + b_0 \quad (b_m \neq 0, m \geq 1), \quad h(x) = c_r x^r + \cdots + c_0 \quad (c_r \neq 0, r \geq 1).$$

Then $a_0 = b_0 c_0$, so either b_0 or c_0 is a multiple of p. Suppose that $p \mid b_0$ and $p \nmid c_0$. Now, $a_1 = b_1 c_0 + c_1 b_0$, so $p \mid b_1 c_0$ and $p \mid b_1$. Similarly, $a_2 = b_2 c_0 + b_1 c_1 + b_0 c_2$, so $p \mid b_2$. Inductively, $p \mid b_i$ for all $i = 0, \ldots, m$. Then $a_n = b_m c_r$ is divisible by p, contradiction. □

Example. We want to check if $25x^5 - 9x^4 - 3x^2 - 12 \in \mathbb{Q}[x]$ is irreducible. We consider the polynomial in $\mathbb{Z}[x]$. For $p = 3$, we can use Eisenstein's criterion and conclude that the polynomial is irreducible.

Corollary. Polynomial $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Q}[x]$ is irreducible for any prime p.

Proof. For $p = 2$, trivial. For $p \geq 3$, we use a trick and check that $\Phi_p(x + 1)$ is irreducible instead. Then we see that

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + px^{p-2} + \binom{p}{2} x^{p-3} + \cdots + p.$$

By Eisenstein's criterion, $\Phi_p(x + 1)$ is irreducible. □

Definition. (Cyclotomic Polynomial) $\Phi_p(x)$ is called the **p-th cyclotomic polynomial**.

Uniqueness of Factorization in $F[x]$

Theorem. Let $p(x) \in F[x]$ be irreducible, and let $r(x), s(x) \in F[x]$. If $p(x) \mid r(x)s(x)$, then $p(x) \mid r(x)$ or $p(x) \mid s(x)$.

Proof. Next class. □

Corollary. Let $p(x) \in F[x]$ be irreducible, $r_1(x), \ldots, r_n(x) \in F[x]$. If $p(x) \mid r_1(x) \cdots r_n(x)$, then $p(x) \mid r_1(x)$ or $p(x) \mid r_2(x)$ or ... or $p(x) \mid r_n(x)$.

We consider irreducible polynomials to be polynomials with degree at least 1.

Theorem. Let $f(x) \in F[x]$ be a nonzero polynomial.

(1) $f(x)$ can be factored into a product of irreducible polynomials.

(2) Irreducible polynomials are unique up to order and unit factors.

Proof. (1) If $f(x)$ is reducible, $f(x) = p(x)q(x)$. Inductively, if $p(x)$,$q(x)$ are reducible, we can factorize it again. But $\deg f < \infty$, this process is finite.

(2) Suppose $f(x) = p_1(x) \cdots p_r(x) = q_1(x) \cdots q_s(x)$ where $p_i(x), q_j(x)$ are irreducible. Since $p_i(x) \mid q_1(x) \cdots q_s(x)$, so $p_i(x) \mid q_1(x)$ or ... or $p_i(x) \mid q_s(x)$. Also, $q_j(x) \mid p_1(x) \cdots p_r(x)$, so $q_j(x) \mid p_1(x)$ or ... or $q_j(x) \mid p_r(x)$. Without loss of generality, let $p_1(x) \mid q_1(x)$. But $q_1(x)$ is irreducible, so $c_1 p_1(x) = q_1(x)$ where c_1 is a nonzero constant. Then we can use the cancellation law and we have

$$p_2(x) \cdots p_r(x) = c_1 q_2(x) \cdots q_s(x).$$

Similarly, repeat the process for $p_2(x), \ldots, p_r(x)$. Then we have $1 = c_1 \cdots c_r q_{r+1}(x) \cdots q_s(x)$. Thus, $r = s$ and $c_1, \ldots, c_r$ are units. □

Remark. The WLOG $p_1(x) \mid q_1(x)$ part accounts for the uniqueness up to order. Also, c_i are all nonzero, so they are units.

Part V

Ideals and Factor Rings

Section 26. Homomorphisms and Factor Rings

Theorem. Given a ring homomorphism $\varphi : R \to R'$,

(1) $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$.

(2) If $S \leq R$, then $\varphi(S) \leq R'$.

(3) If $S' \leq R'$, then $\varphi^{-1}(S') \leq R$.

(4) If $1 \in R$, then $\varphi(1)$ is a unity in $\varphi(R)$.

Proof. Trivial. □

Definition. (Kernel) Given a ring homomorphism $\varphi : R \to R'$, define the **kernel** of φ as

$$\ker \varphi = \varphi^{-1}(0) = \{r \in R : \varphi(r) = 0\}.$$

Theorem. Given a ring homomorphism $\varphi : R \to R'$, let $H = \ker \varphi$. Then

$$\varphi^{-1}(\varphi(a)) = a + H = H + a.$$

Corollary. Ring homomorphism $\varphi : R \to R'$ is a injective if and only if $\ker \varphi = \{0\}$.

Quotient Ring

Theorem. Given a ring homomorphism $\varphi : R \to R'$, let $H = \ker \varphi$. Then R/H is a ring where the binary operations are defined as

$$(a + H) + (b + H) = (a + b) + H, \quad (a + H)(b + H) = ab + H.$$

In addition, $\mu : R/H \to \operatorname{im} \varphi$ is a ring isomorphism.

Proof. It is trivial for addition, since we can apply the results from group theory. So for multiplication, we check well-definedness, associativity, and the distributive law.

For well-definedness, suppose that $a' \in a + H$, $b' \in b + H$. Let $a' = a + h_1$, $b' = b + h_2$, then $a'b' = ab + ah_2 + h_1b + h_1h_2$. Now check that $ah_2 + h_1b + h_1h_2 \in H = \ker \varphi$, so $a'b' \in ab + H$.

Now the rest is trivial, using the well-defined operation.

$$((a + H)(b + H))(c + H) = ((ab)c) + H = (a(bc)) + H = (a + H)((b + H)(c + H)).$$

Finally, μ is definitely a homomorphism, and is surjective if we take $a + H$ for $\varphi(a)$. Also, $\ker \mu = 0 + H$, so it is injective. μ is an isomorphism. □

What property of $\ker \varphi$ allows us to define factor rings?

Theorem. For ring R, let $H \leq R$. The binary operation

$$(a + H)(b + H) = ab + H, \quad (a, b \in R)$$

is a well-defined binary operation on R/H if and only if $ah, hb \in H$ for all $a, b \in R$, $h \in H$.

Proof. Homework. □

Definition. (Ideal) Let N be an additive subgroup of ring R. If $aN \subset N$, $Nb \subset N$ for all $a, b \in R$, the subgroup N is called an **ideal** of R. We will write $N \trianglelefteq R$.[1]

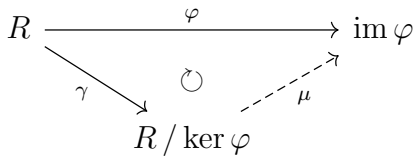
Remark. $aN \subset N$, $Nb \subset N$ for all $a, b \in R$ implies that $N \leq R$.

Definition. (Quotient Ring) If $N \trianglelefteq R$, $(R/N, +, \cdot)$ is a ring with the binary operations defined as

$$(a + N) + (b + N) = (a + b) + N, \quad (a + N)(b + N) = ab + N.$$

This ring is called the **quotient ring** of R by N.

Theorem. (First Isomorphism Theorem) Given a ring homomorphism $\varphi : R \to R'$, $\mu : R \,/\, \ker \varphi \to \operatorname{im} \varphi$ is an isomorphism.



Our conclusion today is that ideals in ring theory is an equivalent concept to normal subgroups in group theory.

[1] Note that this notation doesn't seem to be a standard notation.

May 31st, 2023

Section 27. Prime and Maximal Ideals

We assume that R is a ring with unity.

Definition. Let R be a ring and $N \trianglelefteq R$.

(1) $N \subsetneq R$ is a **proper ideal**.

(2) $N \neq \{0\}$ is a **nontrivial ideal**.

Example. $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$. Most of the examples from abelian groups apply.

Theorem. Let R be a ring and let N be an ideal with a unit. Then $N = R$.

Proof. Let $u \in N$ be a unit. Then $uu^{-1} \in N$, so $1 \cdot r \in N$ for all $r \in R$. $N = R$. □

Corollary. A field contains no proper nontrivial ideals.

Proof. If an ideal of a field contains a nonzero element, it is a unit, so that ideal cannot be proper. □

Definition. (Maximal Ideal) M is a **maximal ideal** of a ring R if M is a proper ideal and there are no proper ideals N such that $M \subsetneq N$.

Theorem. Let R be a commutative ring with unity. Then M is a maximal ideal if and only if $R \,/\, M$ is a field.

Proof. ($\Longrightarrow$) For any $r \notin M$, any ideal containing r and M should equal R. Then $\overline{r} \in R/M$, the ideal containing $\overline{r}$ in R/M is R/M. So there exists $\overline{r'} \in R/M$ such that $\overline{rr'} = 1$.

($\Longleftarrow$) Suppose that M is not maximal. Then there exists a proper ideal N such that $M \subsetneq N$. Then $\varphi(N) \subset R/M$ is a nontrivial proper ideal of R/M. Thus R/M is not a field. □

The main idea is that for the natural projection $\varphi : R \to R/M$, if $I \trianglelefteq R$, then $\varphi(I) \trianglelefteq R/M$. We have used the following lemma in the above proof.

Lemma. Let $\varphi : R \to R'$ be a ring homomorphism.

(1) If $N \trianglelefteq R$, then $\varphi(N) \trianglelefteq \varphi(R)$.

(2) If $N' \trianglelefteq \varphi(R)$ or $N' \trianglelefteq R'$, then $\varphi^{-1}(N') \trianglelefteq R$.

Proof. (2) Take $x \in \varphi^{-1}(N')$ and set $\varphi(x) = n' \in N'$. For $a \in R$, $\varphi(ax) = \varphi(a)\varphi(x) \in N'$, since N' is an ideal. So $ax \in \varphi^{-1}(N')$. □

Example. $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$, so $\mathbb{Z}_n$ is a field if and only if $n\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$. Since $\mathbb{Z}_n$ is a field if and only if n is prime, we conclude that $p\mathbb{Z}$ are the maximal ideals of $\mathbb{Z}$.

Recall the definitions of prime numbers in $\mathbb{Z}$. p is prime if and only if $p \mid ab$ for $a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$. We translate this into the language of ideals.

Definition. (Prime Ideal) Let R be a commutative ring with unity. A proper ideal N is a **prime ideal** if $ab \in N$ then $a \in N$ or $b \in N$. $(a, b \in R)$

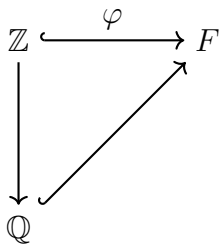
Example. $\{0\}$ is a prime ideal in an integral domain.

Theorem. Let R be a commutative ring with unity. N is a prime ideal if and only if R/N is an integral domain.

Proof. $ab \in N \implies a \in N$ or $b \in N$ if and only if $\overline{ab} = \overline{0} \implies \overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$. □

Corollary. Let R be a commutative ring with unity. If $N \trianglelefteq R$ is maximal, it is also a prime ideal.

Theorem. Let F be a field. If $\operatorname{char} F = p$, $\mathbb{Z}_p \hookrightarrow F$. If $\operatorname{char} F = 0$, $\mathbb{Z} \hookrightarrow F$. Also, $\mathbb{Q}$ is the smallest field containing $\mathbb{Z}$, so F contains a subfield isomorphic to $\mathbb{Q}$.



Proof. Consider $\varphi : \mathbb{Z} \to F$ where $m \mapsto m \cdot 1$, then use the 1st isomorphism theorem. $\mathbb{Q}$ is the field of quotients of $\mathbb{Z}$, so F must contain a subfield isomorphic to $\mathbb{Q}$. □

Thus every field contains either a subfield isomoprhic to $\mathbb{Z}_p$ for some prime p, or a subfield isomorphic to $\mathbb{Q}$. These fields $\mathbb{Z}_p$ and $\mathbb{Q}$ are building blocks.

Definition. $\mathbb{Z}_p$ and $\mathbb{Q}$ are called **prime fields**.

June 5th, 2023

Ideal Structure of $F[x]$

Let F be a field, and let R be a commutative ring with unity. This is a similar concept to cyclic groups in group theory.

Definition. (Principal Ideal) For $a \in R$, $\langle a \rangle = aR$ is called the **principal ideal** generated by a. In addition, an ideal N is prinicpal if there exists an element $a \in R$ such that $N = \langle a \rangle$.

Theorem. Every ideal in $F[x]$ is principal.

Proof. It is trivial that $\langle 0 \rangle = \{0\}$, and $\langle 1 \rangle = F[x]$, so let N be a nontrivial proper ideal of $F[x]$. Take $f(x) \in N$ which has minimal degree in $F[x]$. Then for any $g(x) \in N$, we can find quotient and remainder such that $g(x) = f(x)q(x) + r(x)$, $\deg r < \deg f$ or $r = 0$. Then $r(x) = g(x) - f(x)q(x) \in N$, r has to be 0. Thus $N = \langle f(x) \rangle$. □

Theorem. Ideal $\langle p(x) \rangle \neq \{0\}$ of $F[x]$ is maximal if and only if $p(x)$ is an irreducible polynomial.

Proof. ($\Longrightarrow$) If $p(x)$ is reducible, then there exists $r, s \in F[x]$ with degree at least 1 such that $p(x) = r(x)s(x)$. Then, $p(x) \in \langle r(x) \rangle$, and $\langle p(x) \rangle \subsetneq \langle r(x) \rangle$. So $\langle p(x) \rangle$ is not maximal.

($\Longleftarrow$) Suppose that $\langle p(x) \rangle$ is not maximal. Since all ideals are principal, there exists $r(x) \in F[x]$ such that $\langle p(x) \rangle \subsetneq \langle r(x) \rangle \subsetneq F[x]$. Then $p(x) \in \langle r(x) \rangle$, so $p(x) = r(x)s(x)$ for some $s(x) \in F[x]$. Since $p(x)$ is irreducible, $\deg r = 0$ or $\deg s = 0$. If $\deg s = 0$, then $\langle r(x) \rangle = \langle p(x) \rangle$. If $\deg r = 0$, $r(x)$ is a nonzero constant in F, so it is a unit and $\langle r(x) \rangle = N = F[x]$. Contradiction. □

Theorem. Suppose that $p(x) \in F[x]$ is irreducible. If $p(x) \mid r(x)s(x)$, then $p(x) \mid r(x)$ or $p(x) \mid s(x)$.

Proof. By the above theorem, $\langle p(x) \rangle$ has to be maximal. But maximal ideals are prime. So if $p(x) \mid r(x)s(x)$, $r(x)s(x) \in \langle p(x) \rangle$. Thus $r(x) \in \langle p(x) \rangle$ or $s(x) \in \langle p(x) \rangle$, which implies $p(x) \mid r(x)$ or $p(x) \mid s(x)$. □

Remark. If $p(x) \in F[x]$ is irreducible, $\langle p(x) \rangle$ is maximal, so $E = F[x] / \langle p(x) \rangle$ is a field. Then F is isomorphic to a subfield of E. For example, $\mathbb{R}[x] / \langle x^2 + 1 \rangle \simeq \mathbb{R} \oplus \mathbb{R}$ as a vector space, where $r \mapsto (r, 0)$, $rx \mapsto (0, r)$. Also, it is isomorphic to $\mathbb{C}$ as fields. This will be saved for the next semester. E is called the **extension field** of F and contains zeros of $p(x)$.

Section 38. Free Abelian Groups

What does *free* mean? Suppose that we have a single element 1 and we want to construct an abelian group only with this element. Then we would have $\mathbb{Z}$. If we had an element a, then na, $-na$ ($n \in \mathbb{N}$) would be an element and we get an abelian group $\mathbb{Z}a$. How about for two elements a, b? We would have $\mathbb{Z}a + \mathbb{Z}b$.

In short, *free* means that other than the abelian group and the elements a, b no other relations are required for the group. For example, $a + b$ is just $a + b$, not replaced by another element.

Theorem. Let G be a nontrivial abelian group, $X \subset G$. The following are equivalent.

(1) $\forall a \in G$ can be uniquely expressed by $a = n_1x_2 + n_2x_2 + \cdots + n_rx_r$, where $x_i \in X$ and $n_i \in \mathbb{Z} \setminus \{0\}$.[2]

(2) $\langle X \rangle = G$, $n_1x_1 + \cdots + n_rx_r = 0$ for distinct $x_i \in X$ if and only if $n_1 = \cdots = n_r = 0$.

Proof. Trivial. □

Remark. The condition in (2) seems somewhat similar to the condition of linearly independent vectors. Recall that in linear algebra, if $\mathfrak{B} = \{x_1, \ldots, x_r\}$ is a basis of V, then

$$V = x_1\mathbb{R} \oplus \cdots \oplus x_r\mathbb{R} \simeq \mathbb{R} \oplus \cdots \oplus \mathbb{R} \simeq \mathbb{R}^r,$$

so $\dim V$ is all we needed to classify vector spaces. The free abelian groups also satisfy this kind of property. They have some kind of *basis*.

Definition. (Free Abelian Group) If an abelian group G satisfies the conditions in the above theorem, G is called a **free abelian group**, and the set X is called a **basis**.

Example.

(1) $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ is a free abelian group. The basis is $\{(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\}$. Note that the basis is not unique, as it was in vector spaces.

(2) $\mathbb{Z}_n$ is not free, since $nx = 0$ for all $x \in \mathbb{Z}_n$.

Theorem. Let G be a free abelian group with r basis elements. Then $G = \mathbb{Z}^r$.

Proof. Let $X = \{x_1, \ldots, x_r\}$ be a basis of G. Consider a group homomorphism $\varphi : G \to \mathbb{Z}^r$ as $nx_i \mapsto (0, \ldots, n, 0, \ldots, 0)$. ($n$ is in the i-th component) Then φ is an isomorphism. □

[2] Uniqueness is up to order, and 0 is excluded for uniqueness.

Theorem. Let G be a free abelian group with finiate basis. Then any basis of G has the same number of elements.

Proof. Suppose that $G \simeq \mathbb{Z}^r \simeq \mathbb{Z}^s$ with $r \neq s$. Then $G \,/\, 2G \simeq \mathbb{Z}^r \,/\, 2\mathbb{Z}^r \simeq \mathbb{Z}^s \,/\, 2\mathbb{Z}^s$. But $\mathbb{Z}^r \,/\, 2\mathbb{Z}^r$ has order 2^r, while $\mathbb{Z}^s \,/\, 2\mathbb{Z}^s$ has order 2^s. But $2^r \neq 2^s$, so cannot be isomorphic. □

These are very similar things we did in linear algebra. For vector space V, the basis is not unique, but all bases have the same number of elements, and we called it the *dimension* of a vector space. But in group theory, we give the name *rank*. The above theorem shows that the rank is well-defined.

Definition. (Rank) Let G be a free abelian group. Then the **rank** of G is the number of elements in a basis of G.

Proof of Fundamental Theorem of Abelian Groups

Recall. Let G be a finitely generated abelian group. Then

$$G \simeq \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \tag{$*$}$$

where p_i are primes (not necessarily distinct), $r_i \in \mathbb{N}$, and this representation is unique up to order of products.

Proof. (Sketch) G is finitely generated, so there exists a finite subset $X \subset G$ such that $\langle X \rangle = G$. Suppose that $\langle X \rangle = \{x_1, \ldots, x_n\}$. Consider $\mathbb{Z}^n$ and a group homomorphism $\varphi : \mathbb{Z}^n \to G$ defined as $(a_1, \ldots, a_n) \mapsto a_1 x_1 + \cdots a_n x_n$. φ is well-defined since $\mathbb{Z}^n$ is not a quotient space, and each element is expressed uniquely.

It is enough to show that φ is surjective, so that $\mathbb{Z}^n \,/\, \ker\varphi \simeq G$, and $\mathbb{Z}^n \,/\, \ker\varphi \simeq (*)$. Since $\ker\varphi$ is always a subgroup, we apply the lemma below, and we can show that

$$\mathbb{Z}^n \,/\, \ker\varphi \simeq \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_s} \times \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{n-s}.$$

If we factorize d_i and reorder them, we get the desired expression in $(*)$. □

Lemma. Let G be a nontrivial free abelian group of rank n. If $\{0\} \neq K \leq G$, then K is a free abelian group of rank $s \leq n$, and there is a basis $\{x_1, \ldots, x_n\}$ of G such that $\{d_1 x_1, \ldots, d_s x_s\}$ is a basis of K and $d_i \mid d_{i+1}$.

Proof. Omitted. (Probably next semester?) □