MA672 - (Topics) Number Theory and Cryptography

Jiahua Chen

Spring 2020

These are the course notes for Topics in Advanced Mathematics (**MA672**) at Hotchkiss taught by Dr. Weiss. These notes were last updated January 23, 2020. Any sections denoted with asterisks (***) are currently incomplete, and I will update them when I get to those.

Contents

January 7, 2020

Course Overview

- Abstract algebra: groups, rings, fields.
- Number Theory, arbitrary precision integer arithmetics.
- Cryptographic algorithms

1 Groups

We first define the group, which we will be using extensively.

Definition 1.1. (Group). A group is a set G with a binary operation "$\circ$" such that

- G is closed under $\circ$.
- G is associative.
- There is an Identity Element: $\exists e \in G \mid x \circ e = e \circ x - x \ \forall x \in G$.
- Inverses: $\forall x \in G \ \exists y \in G \mid x \circ y = y \circ x = e$.

Definition 1.2. (Abelian Group). If $\circ$ is commutative in group G, we call G Abelian. In that case, G is often written additively; i.e. we use "+" for "$\circ$".

(If $\circ$ is not commutative, we often write G multiplicatively.)

Definition 1.3. (Subgroup). Let G be a group, and $\emptyset \neq H \subseteq G$. Then H is called a subgroup of G if H is also a group.

A small proof to begin. . .

Proposition 1.4. Let G be a group and $x \in G$. Then x has a unique inverse y, so we can write $y = x^{-1}$.

Proof. Assume y and z are both inverses of x.

$$y = y \circ (x \circ z) = (y \circ x) \circ z = z$$

□

Proposition 1.5. A non-empty subset $H \subseteq G$ is a subgroup of G iff $xy^{-1} \in H \ \forall x, y \in H$.

Proof. ($\Rightarrow$)

- Identity: Pick $x \in H$. Then $xx^{-1} = e \in H$.
- Inverse: If $y \in H$, $ey^{-1} = y^{-1} \in H$

- Closure: If $x, y \in H$, $y^{-1} \in H$, so $x(y^{-1})^{-1} = xy \in H$.

($\Leftarrow$) If H is a group, then $y^{-1} \in H$ (existence of unverse) and $xy^{-1} \in H$ (closure of $\circ$). $\square$

Example:

- Every vector space (without the scalars) is an Abelian group with identity $\vec{0}$.
- Modular arithmetic:
$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$
$\mathbb{Z}_n$ is an Abelian group under modular addition.
$$\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n \mid \gcd(k, n) = 1\}$$
$\mathbb{Z}_n^*$ is an Abelian group under modular multiplication (this is sometimes also $\mathbb{U}_n$).

  Let's take $\mathbb{Z}_4 - \{0\}$ and why it's not a group under multiplication. We can create a multiplication table:

$\circ$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

  However there is no such problem with $\mathbb{Z}_4^*$:

$\circ$	1	3
1	1	3
3	3	1

Definition 1.6. (Cyclic). A group G is called cyclic if $\exists g \in G$ (called generator) such that $G = \{g^n \mid n \in Z\}$.

Example: Z_n are cyclic grous with generator 1.

$\mathbb{Z}_4^*$ is cyclic with generator 3.

Example: The Klein 4-group is not cyclic:

$$K = \{(0,0), (1,0), (0,1), (1,1)\}$$

with componentwise addition mod 2.

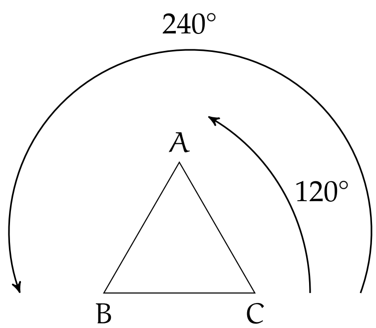
$$K = \mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(k, l) \mid k \in \mathbb{Z}_2, l \in \mathbb{Z}_2\}$$

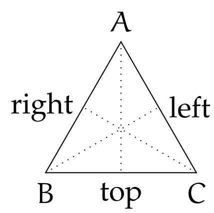
Proposition 1.7. Every cyclic group is Abelian.

Proof. Let $x, y \in G$, a cyclic Abelian group. Let g be the generator in G. We write $x = g^a$ and $y = g^b$. Then $xy = g^a g^b = \underbrace{g \circ g \circ \cdots \circ g}_{k+l \text{ times}} = g^b g^a = yx$. $\square$

Example: The symmetry transformation of an equilateral $\triangle$ form a group under composition.

$$D_3 = \{\mathtt{id}, 120°, 240°, \mathtt{top}, \mathtt{left}, \mathtt{right}\}$$





$\circ$	id	120°	240°	top	left	right
id	id	120°	240°	top	left	right
120°	120°	240°	id	left	right	top
240°	240°	id	120°	right	top	left
top	top	right	left	id	240°	120°
left	left	top	right	120°	id	240°
right	right	left	top	240°	120°	id

Definition 1.8. (Equivalence). Let G be a group and H a subgroup. Define the relation $x \sim y$ if $xy^{-1} \in H$.

Proposition 1.9. $\sim$ is an equivalence relation on G.

If $H = \{e\}$, then $\sim$ is $=$.

If $H = G$, then $\sim$ is trivial.

Proof. We need to show that $\sim$ is

- reflexive: $x \sim x$ for all $x \in G$
$$xx^{-1} = e \in H.$$
- symmetric: $x \sim y \iff y \sim x$ for all $x, y \in G$

  Suppose $x \sim y$. Then $xy^{-1} \in H$. So $(xy^{-1})^{-1} = yx^{-1} \in H \Rightarrow y \sim x$.
- transitive: If $x \sim y, y \sim z$ then $x \sim z$ for all $x, y, z \in G$.

  Suppose $x \sim y, y \sim z$. Then $xy^{-1} \in H, yz^{-1} \in H$. Then $(xy^{-1})(yz^{-1}) = x(y^{-1}y)z^{-1} = xz^{-1} \in H \Rightarrow x \sim z$.

$\square$

If $\sim$ is an equivalence relation on any set X, then $\sim$ partitions X into equivalence classes: If $y \in X, [y] = \{x \in X \mid x \sim y\}$.

Every element of X is in some equivalence class because $\sim$ is reflexive and no two equivalence classes intersect. Consider $[y_1], [y_2]$ and $z \in [y_1] \cap [y_2]$. Then $z \sim y_1$ and $z \sim y_2$ and $y_1 \sim y_2$. Hence, $[y_1] = [y_2]$.

Theorem 1.10. (Lagrange's Theorem). Let G be a finite group of order $|G|$ and H a subgroup of G. Then $|H|$ divides $|G|$.

Proof. We show that the above equivalence relation partitions G into equivalence classes of equal cardinality.

First, notice that H is an equivalence class by itself: $H = [e]$.

Let $[x]$ be another equivalence class. Then $[x] = Hx$: Let $y \in Hx$. Then $\exists a \in H$ such that $y = ax$. Then $\exists a \in H$ such that $y = ax$. But then $yx^{-1} = (ax)x^{-1} = a \in H$, so $y \sim x$.

We need to find a bijection between H and Hx for $x \in G$. Let $f : H \to Hx$, $f(a) = ax$. We ened to show that f is one-to-one and onto:

$$\begin{aligned}
\text{1-1: If } f(a_1) &= f(a_2) \\
a_1 x &= a_2 x \\
a_1 x x^{-1} &= a_2 x x^{-1} \\
a_1 &= a_2.
\end{aligned}$$

Onto: Let $y \in Hx$. Then $\exists a \mid y = ax \Rightarrow y = f(a)$.

$\Rightarrow H \simeq Hx \Rightarrow$ they have the same cardinality.

□

Definition 1.11. (Index). $[G : H]$ is the number of equivalence relations, which is called the index of H in G.

$$[G : H] = \frac{|G|}{|H|}.$$

January 9, 2020

Quick Summary

We were talking about groups, which are

- associative,
- have an identity element,
- and have inverses.

There can be <u>subgroups</u> in groups, a subset of a group that is also a group.

An <u>Abelian group</u> is a commutative group.

A <u>cyclic group</u> is generated by an element g, they're always Abelian.

<u>Lagrange's Theorem</u>: the order of a subgroup divides the order of the group.

<u>Index</u> of H in G: $[G : H] = \frac{|G|}{|H|}$.

Example:

- $(\mathbb{R}^n, +), (\mathbb{C}^n, +)$.
- $(\mathbb{Z}_n, +), (\mathbb{Z}_n^*, \cdot), (\mathbb{R}, +), (\mathbb{R}^*, \cdot), (\mathbb{C}, +), (\mathbb{C}^*, \cdot)$.
- $GL_n(\mathbb{R})$: Invertible $n \times n$ matrices.
- $SL_n(\mathbb{R})$: Subgroup of $GL_n(\mathbb{R})$ with determinant 1.
- $GL_n(\mathbb{C})$: Invertible $n \times n$ complex matrices.
- $U(n)$: Unitary group – determinant of absolute value 1.
- Symmetry groups of geometric shapes. (Dihedral groups)
- Frieze groups.
- Wallpaper groups.
- Crystallographic groups.
- Permutation groups of $\{1, \dots, n\}$ under composition (S_n), and its subgroups.

We will be focusing mainly on $(\mathbb{Z}_n, +), (\mathbb{Z}_n^*, \cdot)$.

Definition 1.12. (Order of an element). Let G be a group and $g \in G$. Then the <u>order</u> of $o(g)$ is the smallest positive integer n such that $g^n = e$. (May be infinite)

Proposition 1.13. Every group of prime order is cyclic.

Proof. Let $e \neq g \in G$. Consider the subgroup $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ generated by g. Then $|\langle g \rangle|$ divides $|G|$, which is prime. Hence $\langle g \rangle = G$. □

1.1 Exercises

Exercise 1. Show that $\{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ is a subgroup of S_4.

Proof. We can construct a Cayley table for the subgroup. (Top row is evaluated first).

$\circ$	(1)	$(1,2)(3,4)$	$(1,3)(2,4)$	$(1,4)(2,3)$
(1)	(1)	$(1,2)(3,4)$	$(1,3)(2,4)$	$(1,4)(2,3)$
$(1,2)(3,4)$	$(1,2)(3,4)$	(1)	$(1,4)(2,3)$	$(1,3)(2,4)$
$(1,3)(2,4)$	$(1,3)(2,4)$	$(1,4)(2,3)$	(1)	$(1,2)(3,4)$
$(1,4)(2,3)$	$(1,4)(2,3)$	$(1,3)(2,4)$	$(1,2)(3,4)$	(1)

Every element is its own inverse, and (1) is the identity element. It is evident from the table that we also have closure. Hence, the set is a valid subgroup under composition. $\square$

Exercise 2. Let G be an Abelian group. Show that the set of all elements of G of finite order forms a subgroup of G.

Proof. Let H be the subset of G with elements of finite order. We want to show that $\forall x, y \in H$, $xy^{-1} \in H$. In other words, xy^{-1} also has finite order. Well, xy^{-1} has order at most $k = \operatorname{lcm}(o(x), o(y))$ such that

$$\begin{aligned}(xy^{-1})^k &= x^k(y^{-1})^k \\ &= x^k(y^k)^{-1} \\ &= e \cdot e^{-1} \\ &= e\end{aligned}$$

Thus, H is a subgroup of G. $\square$

Exercise 3. Let G be a group. Define the set $Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$ of all elements that commute with every other element of G is called the center of G.

(a) Show that $Z(G)$ is a subgroup of G.

(b) Show that $Z(G) = \cap_{a \in G} C(a)$.

(c) Compute the center of S_3.

Proof. (a) e by definition commutes with every other element. $\forall x, y \in Z(G)$, $xy \in Z(G)$ as x, y commutes with every element.

$$(xy)a = x(ya) = x(ay) = (ay)x = a(yx) = a(xy)$$

Inverses also exist as

$$x^{-1}a = (a^{-1}x)^{-1} = (xa^{-1})^{-1} = ax^{-1}$$

(b) If an element is in the intersection of all those sets, then it commutes with every element.

(c) Realize this is simply D_3, where only the identity commutes with one another. *Answer:* $\boxed{\{e\}}$

$\square$

January 10, 2020

Exercise 4. Show that a non-Abelian group must have at least five distinct elements.

Proof. 1 element is trivial. 2 and 3 are primes so all groups of order 2 or 3 are cyclic. So we turn to groups of order 4. Every element cannot have order 1, and shown previously the orders have to divide 4. Additionally, if an element has order 4, then it is a generator and the group is cyclic. So all non-trivial elements must have order 2. We can construct a Cayley table for this specific group.

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Which gives us an Abelian group. □

Exercise 5. Let G be a group. Prove that $(ab)^n = a^n b^n$ for all $a, b \in G$ and all $n \in \mathbb{Z}$ if an only if G is Abelian.

Proof. The left implication is trivial (rearrange). We focus on the right implication.

We let $n = 2$. Then

$$\begin{aligned} (ab)^2 &= a^2 b^2 \\ abab &= aabb \\ a^{-1}babb^{-1} &= a^{-1}aabbb^{-1} \\ ba &= ab \end{aligned}$$

For all $a, b \in G$. □

Exercise 6. Let G be a group. Prove that G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

Proof.

$$\begin{aligned} (ab)^{-1} &= a^{-1}b^{-1} \\ (b^{-1}a^{-1})^{-1} &= (a^{-1}b^{-1})^{-1} \\ ab &= ba \end{aligned}$$

We can travel in both directions in this proof. □

Exercise 7. Let G be a group. Prove that if $x^2 = e$ for all $x \in G$, then G is Abelian.

Proof. We use the fact that $x^{-1} = e$ for all $x \in G$. Then we use the conclusion arrived at *Exercise 6* to our advantage.

$$ab = ab$$
$$(ab)^{-1} = a^{-1}b^{-1}$$

Which is as desired. □

Exercise 8. Show that if G is a finite group with an even number of elements, then there must exist an element $a \in G$ with $a \neq e$ such that $a^2 = e$.

Proof. Assume otherwise, that except for the identity, we can pair elements off such that their inverse isn't themselves. This gives us pairs and the identity, which means the group has an odd number of elements. So there has to be an element whose inverse is itself. □

Exercise 9. Let G be a group, and let $a \in G$. The set $C(a) = \{x \in G \mid xa = ax\}$ of all elements of G is called the <u>centralizer</u> of a.

(a) Show that $C(a)$ is a subgroup of G.

Let $x, y \in C(a)$. Consider

$$\begin{aligned}(xy)a &= x(ya)\\ &= x(ay)\\ &= (ax)y\\ &= a(xy)\end{aligned}$$

So $C(a)$ is closed. We now show that inverses exist:

$$x^{-1}a = x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} = ax^{-1}$$

So $xx^{-1} \in C(a)$ so $C(a)$ is a group.

(b) Show that $\langle a \rangle \subseteq C(a)$.

$\langle a \rangle$ is cyclic and therefore Abelian, so all elements commute with a.

(c) Compute $C(a)$ if $G = S_3$ and $a = (1, 2, 3)$.

(d) Compute $C(a)$ if $G = S_3$ and $a = (1, 2)$.

January 10, 2020

1.2 Group Homomorphisms

Definition 1.14. (Group Homomorphism). Let G_1, G_2 be groups. Then $\varphi : G_1 \longrightarrow G_2$ is called a <u>group homomorphism</u> if

$$\varphi(xy) = \varphi(x)\varphi(y) \tag{1.1}$$

for all $x, y \in G_1$.

Definition 1.15. (Additional Terminology). There are some additional classifications of homomorphisms:

φ is called an <u>isomorphism</u> if φ is 1-1 and onto.

φ is called <u>automorphism</u> if φ is an isomorphism and $G_1 = G_2$

Definition 1.16. (Kernel and Image). Similar to linear algebra and linear transformations, we have <u>kernel</u> and <u>image</u>.

$$\ker\varphi \stackrel{\text{def}}{=} \{x \in G_1 \mid \varphi(x) = e_2\} \text{ where } e_2 \text{ is the identity in } G_2$$
$$\operatorname{im}\varphi \stackrel{\text{def}}{=} \{\varphi(x) \mid x \in G_1\}$$

We call G_2 the "codomain" of φ.

Proposition 1.17. Let $\varphi : G_1 \to G_2$ be a homomorphism. e_1 the identity of G_1 and e_2 the identity of G_2. Then

(i) $\varphi(e_1) = e_2$,

(ii) $\varphi(x^{-1}) = \varphi(x)^{-1}$ for all $x \in G_1$.

Proof. We use the homomorphism definition.

(i) $\varphi(e_1) \cdot \varphi(e_1) = \varphi(e_1^2) = \varphi(e_1) = \varphi(e_1) \cdot e_2 \Rightarrow \varphi(e_1) = e_2$

(ii) $\varphi(x^{-1}) \cdot \varphi(x) = \varphi(x^{-1} \cdot x) = \varphi(e_1) = e_2 \Rightarrow \varphi(x^{-1}) = \varphi(x)^{-1}$

□

Proposition 1.18.

(i) $\ker\varphi$ is a subgroup of G_1,

(ii) $\operatorname{im}\varphi$ is a subgroup of G_2.

Proof.

(i) Let $x, y \in \ker\varphi$. Then $\varphi(xy) = \varphi(x)\varphi(y) = e_2 \cdot e_2 = e_2 \Rightarrow xy \in \ker\varphi$.

(ii) Let $u, w \in \operatorname{im}\varphi$ such that $\varphi(x) = u, \varphi(y) = w$. This implies $uw = \varphi(x)\varphi(y) = \varphi(xy) \Rightarrow uw \in \operatorname{im}\varphi$.

□

We also state the following without proof:

- The inverse of an isomorphism is an isomorphism.
- The composition of isomorphisms is an isomorphism.

- We say $G_1 \cong G_2$ if there exists an isomorphism $\varphi : G_1 \leftrightarrow G_2$, and isomorphisms of groups in an equivalence relation.

1.3 Exercises

Exercise 10. Let G be the following set of matrices over $\mathbb{R}$:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

Show that G is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. We can construct the map

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mapsto (0,0), \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \mapsto (0,1), \quad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \mapsto (1,0), \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \mapsto (1,1)$$

Constructing a Cayley table (or simple trial and error) shows that this is a valid isomorphism. Another things we could note is that the only groups with 4 elements are isomorphisms of $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. Noting that the matrices aren't cyclic (there is no generator) also gives the compatible conclusion. □

Exercise 11. Let G be any group. and let a be a fixed element of G. Define a function $\phi_a : G \to G$ by $\phi_a(x) = axa^{-1}$, for all $x \in G$. Show that ϕ_a is an isomorphism.

Proof. We first show that ϕ_a is a bijection by proving that it's 1-1 and onto:

$$\begin{aligned} \phi_a(x) &= \phi_a(y) \\ axa^{-1} &= aya^{-1} \\ x &= y \end{aligned}$$

Let $w \in G$. Then $\phi_a(a^{-1}wa) = aa^{-1}waa^{-1} = w$.

We now show that ϕ_a is a homomorphism:

$$\phi_a(x)\phi_a(y) = axa^{-1}aya^{-1} = axya^{-1} = \phi_a(xy)$$

□

Proposition 1.19. Let $\varphi \in \mathrm{Hom}(G_1, G_2)$. Then φ is 1-1 iff $\ker \varphi = \{e_1\}$.

Proof. ($\Rightarrow$) If φ is 1-1, and $x \in \ker \varphi$,

$$\varphi(x) = \varphi(e_1) = e_2 \Rightarrow x = e_1$$

($\Leftarrow$) If $\ker \varphi = \{e_1\}$ and

$$\begin{aligned} \varphi(x) &= \varphi(y) \\ \varphi(x)\varphi(y)^{-1} &= e_2 \\ \varphi(x)\varphi(y^{-1}) &= e_2 \\ \varphi(xy^{-1}) &= e_2 \\ xy^{-1} &= e_1 \\ x &= y \end{aligned}$$

□

Exercise 12. Show that the multiplicative group $\mathbb{Z}_7^*$ is isomorphic to the additive group $\mathbb{Z}_6$.

Proof. By trial and error, we find that 3 is a generator in $\mathbb{Z}_7^*$.

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1$$

So we map powers of 3 to its powers which is an isomorphism. □

January 14, 2020

Exercise 13.

(a) Write down the formulas for all homomorphisms from $\mathbb{Z}_6$ into $\mathbb{Z}_9$.

We can list all the subgroups of $\mathbb{Z}_6$ (recall a kernel has to be a subgroup). Then try to find a homomorphism for each subgroup.

- $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} : \varphi(m) \equiv 0$
- $\{0\}$: cannot be kernel because there is no subgroup of order 6 in $\mathbb{Z}_9$
- $\{0, 2, 4\}$: cannot be kernel
- $\{0, 3\} : \varphi(m) = 3m$

(b) Do the same for all homomorphisms from $\mathbb{Z}_{24}$ into $\mathbb{Z}_{18}$.

We can attempt to solve this problem in the general sense, classifying all homomorphisms from $\mathbb{Z}_m$ to $\mathbb{Z}_n$. Realize that the generator of the kernel in $\mathbb{Z}_{24}$ must get sent to 0, i.e. $\equiv 0 \mod 18$. This means that any generator must be a common divisor of 24 and 18, of which there are $1, 2, 3,$ and 6. We construct the homomorphism by creating $\varphi(m) = km, k = \frac{18}{g}$ where g is a generator for the kernel. We can extend this to m and n.

Exercise 14. Show that $\phi_3 : \mathbb{Z}_3 \to \mathbb{Z}_3$ defined by $\phi_3([x]) = [x]^3$ and $\phi_5 : \mathbb{Z}_5 \to \mathbb{Z}_5$ defined by $\phi_5([x]) = [x]^5$ are homomorphisms but $\phi_4 : \mathbb{Z}_4 \to \mathbb{Z}_4$ defined by $\phi_4([x]) = [x]^4$ is not.

Proof. We can use the freshman dream lemma:

$$(x + y)^p \equiv x^p + y^p \mod p$$

Which makes any ϕ_p a homomorphism. □

Exercise 15. Let G be an Abelian group, and let n be any positive integer. Show that the function $\phi : G \longrightarrow G$ defined by $\varphi(x) = nx$ is a homomorphism.

Proof. We write

$$\varphi(x) + \varphi(y) = nx + ny = \underbrace{x + \cdots + x}_{n \text{ times}} + \underbrace{y + \cdots + y}_{n \text{ times}} = \underbrace{(x + y) + \cdots + (x + y)}_{n \text{ times}} = \varphi(x + y)$$

□

Exercise 16. Show that $\varphi : \mathbb{C}^{\times} \longrightarrow \mathbb{R}^{\times}$ defined by $\varphi(a + bi) = a^2 + b^2$ is a homomorphism.

Proof. We can write it in $e^{i\theta}$ form to make out life easier (otherwise it's algebra and a lot of foiling).

$$\varphi(re^{i\alpha}se^{i\beta}) = \varphi(rse^{i(\alpha+\beta)}) = r^2s^2$$

□

Exercise 17. Let ϕ be a group homomorphism of G_1 onto G_2. Prove that:

1. If G_1 is Abelian then so if G_2.

   Let $u, w \in G_2$, $\varphi(x) = u$, $\varphi(y) = w$ (φ is onto)

   $$u + w = \varphi(x) + \varphi(y) = \varphi(x + y) = \varphi(y + x) = \varphi(y) + \varphi(x) = w + u$$

   Counterexample: $\det : GL_2(\mathbb{R}) \longrightarrow \mathbb{R}^{\times}$

2. If G_1 is cyclic then so is G_2.

   We take the generator $g_1 \in G_1$ and claim it is also a generator $\varphi(g_1) = g_2 \in G_2$.

   Counterexample: $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$, $\varphi(m, n) = m$.

   Here's another nice counterexample: $\varphi : GL_2(\mathbb{R}) \longrightarrow \{1\} \subseteq \mathbb{R}^{\times}$.

3. Give a counterexample to the converse of the statement.

Definition 1.20. (Normal Subgroups). Let H be a subgroup of G. H is called normal if ghg^{-1} for all $g \in G$, $h \in H$.

$$gHg^{-1} \subseteq H \tag{1.2}$$

Proposition 1.21. Let $\phi : G_1 \longrightarrow G_2$ be a group homomorphism.

(a) If H_1 is a subgroup of G_2, then $\phi(H_1)$ is a subgroup of G_2. If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2) = \{x \in G_1 \mid \phi(x) \in H_2\}$ is a subgroup of G_1. If H_2 is normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

Let's do a quick exercise that involves normal subgroups:

Exercise 18. Recall that the center of a group G is $\{x \in G \mid xg = gx \text{ for all } g \in G\}$. Prove that the center of any group is a normal subgroup.

Proof. Take $x \in Z(G)$ and $g \in G$.

$$gxg^{-1} = xgg^{-1} = x \in Z(G)$$

$\square$

January 16, 2020

(***)

January 17, 2020

(***)

January 18, 2020

(***)

January 21, 2020

2 Rings

2.1 Recap

Recall the characteristics of a ring:

- 2 operations $+$ and $\cdot$.
- Abelian group w.r.t. $+$.
- Closure under $\cdot$.
- Distributive law of multiplication over addition.

Some additional characterizations of rings include:

- Commutative ring with identity.
  - $\cdot$ has identity 1.
  - $\cdot$ is commutative.
- $(\mathbb{R}^*, \cdot)$ is an Abelian group: field.
- If $rs = 0$ implies $r = 0$ or $s = 0$: integral domain.
- Integral domain and existence of a long division algorithm: Euclidian domain. e.g. integers, polynomials.
- Ideal: $I \subseteq R$ such that

- $a + b \in I \ \forall a, b \in I$.
- $ar \in I \ \forall a \in I, r \in R$.

Ex: $\langle a \rangle = \{ar : r \in R\}$ for some $a \in R$, commutative.

Definition 2.1. (Ideals). Let I be a proper (non-trivial) ideal in a commutative ring R.

- I is called prime ideal if for all $a, b \in R$, $ab \in I \Rightarrow a \in I$ or $b \in I$.
- I is called maximal ideal if for all ideals J with $I \subseteq J \subseteq R$, $J = I$ or $J = R$.

Definition 2.2. (Ring Homomorphism). Let R and S be commutative rings. A function $\phi : R \longrightarrow S$ is called a ring homomorphism if

$$\phi(a + b) = \phi(a) + \phi(b) \tag{2.1}$$

and

$$\phi(ab) = \phi(a)\phi(b) \tag{2.2}$$

for all $a, b \in R$.

A ring homomorphism that is one-to-one and onto is called an isomorphism. If there exists an isomorphism from R onto S, we say R is isomorphic to S, and write $R \cong S$.

Proposition 2.3. Let $\phi : R \longrightarrow S$ be a ring homomorphism. Then

(a) $\phi(0) = 0$;

(b) $\phi(-a) = -\phi(a)$ for all $a \in R$;

(c) If 1 is an identity element for R, then $\phi(1)$ is an idempotent element of S.

(d) $\phi(R)$ is a subring of S.

Proof.

(a) This is true as ϕ is a group homomorphism.

(b) Similar to above.

(c) $\phi(1)\phi(1) = \phi(1 \cdot 1) = \phi(1)$.

(d) $\phi(R)$ is a subgroup of S by above. We now show that multiplication is well defined and distributes.

$$\phi(a)\phi(b) = \phi(ab) \in \phi(R) \text{ as } ab \in R$$

$$\phi(a)(\phi(x) + \phi(y)) = \phi(a)\phi(x + y) = \phi(a(x + y))$$

$$= \phi(ax + ay) = \phi(ax) + \phi(ay) = \phi(a)\phi(x) + \phi(a)\phi(y) \in R$$

□

Example: Consider $\mathbb{Z}_n$ with

$$[x] + [y] = [x + y]$$
$$[x][y] = [x][y]$$

Then $\pi : \mathbb{Z} \to \mathbb{Z}_n$ with $\pi(x) = [x]$ is a ring homomorphism.

Proof. C'mon. □

Proposition 2.4. Let $\phi : R \to S$ be a ring homomorphism.

(a) If $a, b \in \ker(\phi)$ and $r \in R$, then $a + b$, $a - b$, and ra belong to $\ker(\phi)$.

(b) The homomorphism ϕ is an isomorphism if and only if $\ker(\phi) = \{0\}$ and $\phi(R) = S$.

Proof. (a) If $a, b \in \ker(\phi)$, then

$$\phi(a \pm b) = \phi(a) \pm \phi(b) = 0 \pm 0 = 0,$$

and so $a \pm b \in \ker(\phi)$. If $r \in R$, then

$$\phi(ra) = \phi(r) \cdot \phi(a) = \phi(r) \cdot 0 = 0,$$

showing that $ra \in \ker(\phi)$.

(b) This part follows from the fact that ϕ is a group homomorphism, since ϕ is one-to-one if and only if $\ker(\phi) = \{0\}$ and onto if and only if $\phi(R) = S$.

□

Definition 2.5. (***). Let R, S be commutative rings. $\varphi : R \to S$ a homomorphism. Then $R/\ker(\varphi) = \{[r] \mid r \in R\}$ where $r \sim s$ if $r - s \in \ker(\varphi)$. (or $\varphi(r) = \varphi(s)$).

Theorem 2.6. $R/\ker(\varphi)$ is a ring, and $R/\ker(\varphi) \cong \operatorname{im}(\varphi)$.

Proof. We already know $R/\ker(\varphi)$ is an Abelian group w.r.t. $+$.

It is closed under multiplication: $[r][s] = [rs]$. Because $rs - rs \in \ker(\varphi)$ ($\varphi(0) = 0$), $[rs] \in R/\ker(\varphi)$.

Distributive law:

$$\begin{aligned}
[r]([s] + [t]) &= [r][s + t] \\
&= [r(s + t)] \\
&= [rs + rt] \\
&= [rs] + [rt] \\
&= [r][s] + [r][t]
\end{aligned}$$

Consider $\psi : R/\ker(\varphi) \to \operatorname{im}(\varphi)$ with $\psi([r]) = \varphi(r)$.

ψ is a (i) ring homomorphism that is (ii) one-to-one and (iii) onto.

(i) $\psi([r]+[s]) = \psi([r+s]) = \varphi(r+s) = \varphi(r)+\varphi(s) = \psi([r])+\psi([s])$.

We prove similarly for multiplication.

(ii) ψ is one-to-one if and only if $\ker\psi = \{[0]\}$.

$$\begin{aligned} \text{Suppose } \psi([r]) &= 0 \\ \varphi(r) &= 0 \\ r &\in \ker\varphi \\ r &\sim 0 \\ r &\in [0] \\ [r] &= [0]. \end{aligned}$$

(iii) Let $w \in \mathrm{im}\varphi$ such that $\varphi(r) = w$. Hence $\psi([r]) = w$.

□

Exercise 1. Let F be a field and let $\phi : F \to R$ be a ring homomorphism. Show that ϕ is either zero or one-to-one.

Proof. Let $\phi : F \to R$ be a ring homomorphism, ϕ not zero.

Then $\ker\phi \subsetneq F$.

Let $a \in \ker\phi$. Let $r \in F$.

$$\phi(r) = \phi(r \cdot 1) = \phi(r \cdot a \cdot a^{-1}) = \phi(r)\phi(a)\phi(a^{-1}) = 0$$

$$\Rightarrow r \in \ker\phi \Rightarrow \ker\phi = F \Rightarrow\Leftarrow$$

□

Exercise 2. Let F, E be fields, with a homomorphism $\phi : F \to E$. Show that if ϕ is onto, then ϕ must also be an isomorphism.

Proof. This follows directly from Exercise 1. □

Exercise 3. Show that taking complex conjugates defines an automorphism of $\mathbb{C}$. That is, for $z \in \mathbb{C}$, define $\phi(z) = \bar{z}$, and show that ϕ is an automorphism.

Proof. (***) □

Exercise 4. Show that the only ring automorphism of $\mathbb{Z}$ is the identity mapping.

Proof. Since $\varphi(1)$ is idempotent, $\varphi(1) = 1$ as 1 is the only non-trivial idempotent integer. We also note that $\varphi(-1) = -\varphi(1) = -1$ and $\varphi(0) = 0$ by group homomorphism. Then we can induct in both directions *to infinity and beyond*. (***) □

Exercise 5. Let R be a commutative ring with identity, and let D be an integral domain. Show that $\phi(1) = 1$ for any nonzero ring homomorphism $\phi : R \to D$.

Proof. (***) □

January 23, 2020

Let R be a ring and $I \subseteq R$ an ideal. Since I is a normal group of $(R, +)$, we can construct the Abelian group

$$R/I = \{r + I \mid r \in R\}.$$

This can be given a ring structure by defining multiplication in the obvious way:

$$[r][s] = [rs]$$

With $[r] = r + I$, $[s] = s + I$, we get

$$\begin{aligned}(r + I)(s + I) &= rs + \underbrace{\underbrace{rI}_{\subseteq I} + \underbrace{sI}_{\subseteq I} + \underbrace{II}_{\subseteq I}}_{=I} \\ &= rs + I \\ &= [rs]\end{aligned}$$

Example: If $\varphi : R \to S$ is a homomorphism, $\ker \varphi$ is an ideal in R, so this is an extension of $R/\ker \varphi$. (***)

Consider $\mathbb{Z}_2[x]/\langle x^2 + 1\rangle$.

Take the ring of polynomials with coefficients in $\mathbb{Z}_2 = \{0, 1\}$ and mod out the ideal generated by $x^2 + 1$:

$$\langle x^2 + 1\rangle = (x^2 + 1) \cdot \mathbb{Z}_2[x]$$

In this, two polynomials $p(x)$ and $q(x)$ are equivalent if $p(x) - q(x) \in (x^2 + 1) \cdot \mathbb{Z}_2[x]$.

$\Rightarrow$ “$p(x) - q(x)$ is divisible by $x^2 + 1$”, or “they have the same remainder under division by $x^2 + 1$.”

The equivalence classes can be represented by the possible remainders under division by $x^2 + 1 \iff$ all polynomials of degree at most 1 are in $\mathbb{Z}_2[x]$.

$$\mathbb{Z}_2[x]/\langle x^2 + 1\rangle = \{0, 1, x, x + 1\}$$

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	1	x	$x+1$
1	1	x	$x+1$
x	x	1	$x+1$
$x+1$	$x+1$	$x+1$	0

Exercise 6. Give a multiplication table for the ring $\mathbb{Z}_2[x]/\langle x^3 + x^2 + x + 1\rangle$.

$\cdot$	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2	x^2+x	x^2+x+1	x^2+1	$x+1$	1
$x+1$	$x+1$	x^2+x	x^2+1	$x+1$	0	x^2+1	x^2+x
x^2	x^2	x^2+x+1	$x+1$	1	x^2+1	x^2+x	x
x^2+1	x^2+1	x^2+1	0	x^2+1	0	0	x^2+1
x^2+x	x^2+x	$x+1$	x^2+1	x^2+x	0	x^2+1	$x+1$
x^2+x+1	x^2+x+1	1	x^2+x	x	x^2+1	$x+1$	x^2

Exercise 7. Let R be a ring and I an ideal. If I contains a unit of R, $I = R$.

Proof. Let $u \in I$ be a unit. Then it has a multiplicative inverse $u^{-1} \in R$. Then $uu^{-1} \in I \Rightarrow 1 \in I$. Then $\forall r \in R, 1 \cdot r = r \in I$. Thus $I = R$. $\square$