PMATH 347: Groups and Rings
Final Summary

Professor Ross Willard
LaTeXer Iris Jiang

Fall 2020

1 Group Theory

Definition 1.1. Binary Operation
Let A be a non-empty set. A **binary operation** on A is a function $*$ whose domain is $A \times A$ (the set of all ordered pairs from A) and which maps into A.

Definition 1.2. Group
A **group** is an ordered pair $(G, *)$, where

- G is a non-empty set
- $*$ is a binary operation on G

which jointly satisfy the following further conditions:

- $*$ is **associative**: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$
- There exists an **identity** element $e \in G$: $a * e = e * a = a$ for all $a \in G$
- Every $a \in G$ has a 2-sided **inverse**. i.e. an element $a' \in G$ which satisfies $a * a' = a' * a = e$

Definition 1.3. Order
The **order** of a group G, denoted $|G|$, is the number of its elements.
For a group G and element $a \in G$, the **order** of a (denoted $|a| or \circ(a)$) is the least integer $n > 0$ such that $a^n = 1$, if it exists. If no such n exists (this requires G to be infinite), then the order of a is defined to be ∞.

Proposition 1.1. *Suppose G is a group, $a \in G$, and $\circ(a) = n < \infty$. Then for all $k \in \mathbb{Z}$, $a^k = 1 \iff n|k$*

Proposition 1.2. *Let G be a group and $a, b, u, v \in G$*

1. *Left and right cancellation*
   (a) *If $au = av$, then $u = v$*
   (b) *If $ub = vb$, then $u = v$*
2. *The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$*

Corollary. *In any group G, the identity element is unique.*

Proposition 1.3. *Suppose G is a group,*

1. *Each $a \in G$ has a unique inverse a^{-1}*
2. *$(a^{-1})^{-1} = a$ for all $a \in G$*
3. *$(ab)^{-1} = (b^{-1})(a^{-1})$ for all $a, b \in G$*

Definition 1.4. Abelian, cyclic, generator
G is **abelian** if $ab = ba$ for all $a, b \in G$
If $a \in G$ then $\langle a \rangle$ denotes the set $\{a^n : n \in \mathbb{Z}\}$. Thus $\langle a \rangle \subseteq G$
G is **cyclic** if there exists $a \in G$ such that $G = \langle a \rangle$, in this case we call a a **generator** of G

2 Ring Theory

Definition 2.1. Ring
A **ring** is an ordered triple $(R, +, \cdot)$ where

- R is a non-empty set
- $+$ and $\cdot$ are binary operations on R

which jointly satisfy the following conditions:

1. $(R, +)$ is an abelian group
2. $\cdot$ is associative
3. There exists $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$
4. (Distributive laws): for all $a, b, c \in R$

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Proposition 2.1. *Let R be a ring. Then*

1. $0a = a0 = 0$ *for all* $a \in R$
2. $-a = (-1)a = a(-1)$ *for all* $a \in R$
3. $(-a)b = a(-b) = -(ab)$ *for all* $a, b \in R$
4. $(-a)(-b) = ab$

Definition 2.2. Unit, invertible, inverse
Let R be a ring.

1. An element $a \in R$ is a **unit** if there exists $b \in R$ satisfying $ab = ba = 1$. (We also say that a is invertible. b is called the **inverse** of a and is denoted a^{-1}; it is provably unique.)
2. $R^\times$ denotes the set of units in R.

Definition 2.3. Division ring, field

1. A **division ring** is a ring D satisfying $0 \neq 1$ and $D^\times = D \backslash \{0\}$
2. A **field** is a commutative division ring

Definition 2.4. Zero divisor
Let R be a ring. A **zero divisor** is an element $a \in R$ such that

1. $a \neq 0$
2. There exists $b \in R$ with $b \neq 0$ such that $ab = 0$ or $ba = 0$ (or both)

Proposition 2.2. *Suppose R is a ring and $a \in R$ with $a \neq 0$. If a is not a zero divisor, then we can "multiplicatively cancel by a." That is for all $b, c \in R$,*

$$ab = ac \implies b = c$$
$$ba = ca \implies b = c$$

Lemma. *If R is a ring and $a \in R^\times$, then a is not a zero divisor. Hence we can always "multiplicatively cancel by units."*

Definition 2.5. integral domain
A ring R is called an **integral domain** (or domain) if it is commutative, satisfies $0 \neq 1$, and has no zero divisors.

Corollary. *Every field is an integral domain.*

Definition 2.6. Subring
Suppose R is a ring. A **subring** of R is a subset $S \subseteq R$ such that

1. S is a subgroup of (R, +)
2. S is closed under multiplication (i.e., $a, b \in S$ implies $ab \in S$)
3. $1 \in S$

Write $S \leq R$ to denote that S is a subring of R

Definition 2.7. $R[x]$ $R[x]$ denotes the set of all polynomials in x over R

Theorem 2.1. *$R[x]$ is a ring containing R as a subring.*

Theorem 2.2. *Suppose $q(x), r(x) \in R[x]$ and let $p(x) = q(x) \cdot r(x)$. If R is commutative, then $p(c) = q(c) \cdot r(c)$ for all $c \in R$*

Definition 2.8. homomorphism
Let R, S be rings. A function $\varphi : R\ toS$ is a **homomorphism** (of rings) if

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$
2. $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$
3. $\varphi(1_R) = 1_S$

Definition 2.9. isomorphism
As in the case of groups

1. An **isomorphism** is a bijective homomorphism
2. Write $R \cong S$ if there exists an isomorphism from R to S

Definition 2.10. Ideal Let R be a ring and $I \subseteq R$

1. I is a **left ideal** of R of
   (a) I is a subgroup of $(R, +)$
   (b) If $r \in R$ and $a \in I$, then $ra \in I$
2. Right deals are defined dually ($a \in I, r \in R \implies ar \in I$)
3. I is an **ideal** if it is both a left and right ideal

Proposition 2.3. *If I is an ideal of R and $1 \in I$, then $I = R$*

Proposition 2.4. *Let R, S be rings and $\varphi : R \to S$ a homomorphism*

1. *$im(\varphi)$ is a subring of S*
2. *$\ker(\varphi)$ is an ideal of R*

Claim. *The rule $(a + I) \cdot (b + I) := (ab) + I$ defines an operation $\cdot$ on R/I*

Claim. *If R is a ring and I is an ideal, then $(R/I, +, \cdot)$ is a ring*

Theorem 2.3. ***First t Isomorphism Theorem for rings***
Suppose R, S are rings and $\varphi : R \to S$ is a surjective homomorphism. Then $R/\ker(\varphi) \cong S$

Definition 2.11. principal ideal
Let R be a ring and $a \in R$

1. $Ra = \{ra : r \in R\}$
2. $aR = \{ar : r \in R\}$
3. (a) denotes the smallest ideal of R containing a. (More precisely, (a) is the intersection of all ideals containing a)

We call (a) the **principal ideal generated by** a

Lemma. *Suppose R is a ring and $a \in R$*

1. *Ra is a left ideal. It is the smallest left ideal of R containing a*
2. *Similarly, aR is the smallest right ideal of R containing a*
3. *$Ra \cup aR \subseteq (a)$*

$(a) = Ra = aR$ if R is commutative.

Lemma. *Suppose I, J are ideals of R*

1. *$I \cup J$ is an ideal; it is the largest ideal of R contained in both I and J*
2. *$I + J := \{a + b : a \in I, b \in J\}$ is the smallest ideal of R containing both I and J*

Definition 2.12. proper, properly contains, maximal ideal
Let R be a ring

1. An ideal I is **proper** if $I \neq R$. (equivalently, if $1 \notin I$)
2. If I, J are ideals, then J **properly contains** I if $I \subseteq J$ and $I \neq J$
3. I is a **maximal ideal** if it is a proper ideal, and the only ideal properly containing it is R

Proposition 2.5. *Suppose R is a commutative ring and I is an ideal. R/I is a field iff I is a maximal ideal.*

Definition 2.13. prime ideal
Suppose R is a commutative ring. An ideal I of R is a **prime ideal** if it is proper and $ab \in I$ implies $a \in I$ or $b \in I$

Proposition 2.6. *Suppose R is a commutative ring and I is an ideal. R/I is an integral domain iff I is a prime ideal.*

Corollary. *Every maximal ideal of a commutative ring is a prime ideal.*

Proposition 2.7. *Let R be a ring. Every proper ideal of R is contained in a maximal ideal of R.*

Definition 2.14. chain of proper ideal
A **chain of proper ideals** is set S of proper ideals with the property that for all $I, J \in S$, either $I \subseteq J$ or $J \subseteq I$. (S can be uncountable)

Lemma. ***Zorn's Lemma***
Suppose $(A, \leq)$ is a set equipped with a partial order. If every chain in $(A, \leq)$ has an upper bound in A, then every element of A lies below a maximal element of A.
(A maximal element is an element $a \in A$ such that $a \leq b \in A$ implies $b = a$)

Definition 2.15. If R is a ring, I is an ideal, and $a, b \in R$, then we write $a \equiv b \pmod{I}$ to mean $a+I = b+I$ (equivalentlym $b - a \in I$)

Definition 2.16. coprime
Let R be a ring. Two ideals I, J are **coprime** of $I + J = R$

Theorem 2.4. *Chinese Remainder Theorem*
Suppose R is a ring and I, J are coprime ideals. Then for all $a, b \in R$ there exists $c \in R$ such that $c \equiv a \pmod{I}$ and $c \equiv b \pmod{I}$

Corollary. *Suppose R is a ring and I, J are coprime ideals*

1. $R/(I \cap J) \cong R/I \times R/J$
2. *If $I \cap J = \{0\}$ then $R \cong R/I \times R/J$*

Proposition 2.8. *Every ideal of $\mathbb{Z}$ is principal.*

Definition 2.17. Principal Ideal Domain (PID)
A ring R is a **Principal Ideal Domain** (PID) if

1. R is an integral domain (commutative, $0 \neq 1$, no zero divisors)
2. Every ideal of R is principal

Lemma. *In a commutative ring R, an element u is a unit iff $u|1$*

Corollary. *In a commutative ring R, u is a unit iff $(u) = (1)$*

Definition 2.18. associates
We say that a and b are **associates** and write $a \sim b$ if $a = ub$ for some unit $u \in R^{\times}$

Lemma. *In an integral domain R, $a \sim b$ iff $a|b$ and $b|a$*

Corollary. *In an integral domain R, $a \sim b$ iff $(a) = (b)$*

Definition 2.19. nontrivial factorization, reducible, irreducible, prime Let R be an integral domain. Assume $a \in R$ with $a \neq 0$ and $a \notin R^{\times}$

1. A **nontrivial factorization** of a is an equation $a = bc$ where $b, c \in R$ and neither b nor c is a unit
2. a is **reducible** if it has a nontrivial factorization in R
3. Otherwise a is irreducible (equivalently, $a = bc$ implies b or c is a unit)
4. We say that a is a **prime** if for all $b, c \in R$, if $a|bc$ then $a|b$ or $a|c$

Proposition 2.9. *In an integral domain, every prime is irreducible.*

Proposition 2.10. *Suppose R is an integral domain and $a \in R$. Then a is irreducible iff $(a) \neq (0)$, $(a) \neq (1)$ and there is no principal ideal (b) properly between (a) and (1)*

Definition 2.20. complete factorization
Suppose R is an integral domain, $a \in R$, $a \neq 0$, and $a \notin R^{\times}$. A **complete factorization** of a is an equation $a = p_1 p_2 \cdots p_n$, where $n \geq 1$, $p_1, p_2, \ldots, p_n \in R$, and each p_i is irreducible.

Proposition 2.11. *Suppose R is an integral domain and R does* **not** *have an infinite strictly increasing chain of principal ideals. Then every $a \in R$ with $a \neq 0$, $a \notin R^{\times}$ has a complete factorization.*

Definition 2.21. essentially the same Let R be an integral domain and $a \in R$ with $a \neq 0$. $a \notin R^{\times}$

1. Two complete factorization of a $a = p_1 p_2 \cdots p_n$ and $a = q_1 q_2 \cdots q_m$ are **essentially the same** provided:
   (a) $m = n$, and

(b) After a suitable re-ordering of the q_i's we have $p_i \sim q_i$ for all $i = 1, \ldots, n$

2. We say that **complete factorization in R are unique, when they exists**, and we write "R has UCF', provided for any $a \in R$ with $a \neq 0$ and $a \notin R^\times$, if a has a complete factorization, then any two complete factorization of a are essentially the same

Lemma. *In an integral domain, if p is a prime and $p|a_1a_2\cdots a_n$, then $p|a_i$ for some i*

Corollary. *Suppose R is an integral domain, $p \in R$ is a prime, and $a = q_1 \cdots q_m$ is a complete factorization of $a \in R$. Then $p|a$ iff $p \sim q_i$ for some i*

Proposition 2.12. *Suppose R is an integral domain in which every irreducible element is prime. Then R has UCF.*

Definition 2.22. Unique Factorization Domain
An integral domain R is a **Unique Factorization Domain** (UFD) if

1. R does not have an infinite strictly increasing chain of principal ideals

2. every irreducible in R is a prime

Lemma. *Let R be an integral domain and $p \in R$ with $p \neq 0$. (p) is a prime ideal iff p is a prime*

Proposition 2.13. *Suppose R is a PID and $p \in R$ with $p \neq 0$. The following are equivalent:*

1. *p is irreducible*

2. *p is a prime*

3. *(p) is a maximal ideal*

Corollary. *Suppose R is a PID and p is an irreducible element in R. Then $R/(p)$ is a field.*

Theorem 2.5. *Every PID is a UFD.*

Corollary. *If F is a field, then $F[x]$ is a UFD.*

Definition 2.23. Greatest Common Divisor
Let R be an integral domain and $a, b, d \in R$. We say that d is a **greatest common divisor** of a and b if

1. d is a common divisor: $d|a$ and $d|b$

2. d is divisible by every common divisor: for all $c \in R$, if $c|a$ and $c|b$, then $c|d$

Lemma. *Suppose R is a UFD. For every finite list $a_1, \ldots, a_n \in R$, if at least one of the a_i's is nonzero, then the list has a greatest common divisor.*

Definition 2.24. relatively prime
Suppose R is an integral domain and $a_1, \ldots, a_n \in R$. We say that $a_1, \ldots, a_n$ are **relatively prime** if the only common divisors of $a_1, \ldots, a_n$ are the units in $R^\times$; equivalently, if 1 is a greatest common divisor of $a_1, \ldots, a_n$

Lemma. *Suppose R is a UFD and $a_1, \ldots, a_n \in R$ with at least one $a_i \neq 0$. Let $d \in R$ be a greatest common divisor of $a_1 \ldots, a_n$. Define $a'_1, \ldots, a'_n \in R$ by $a'_i := d_i/d$ (i.e. a'_i is the unique solution x to $a_i = dx$). Then $a'_1, \ldots, a'_n$ are relatively prime.*

Lemma. *Suppose R is an integral domain and $p \in R$ is a prime in R. Then p is a prime in $R[x]$.*

Lemma. *Suppose R is a UFD, $f(x), g(x) \in R[x]$, and $u \in R$, $u \neq 0$. If $u|f(x)g(x)$, then there exists a factorization $u = cd$ of u in R such that $c|f(x)$ and $d|g(x)$*

Proposition 2.14. ***Gauss' Lemma***
Suppose R is UFD and F is its field of fractions $\{n/d : n, d \in R, d \neq 0\}$. Let $p(x) \in R[x]$ by a polynomial of degree ≥ 1.

Every nontrivial factorization of $p(x)$ in $F[x]$ can be essentially realized in $R[x]$, in the following sense: if $p(x) = A(x)B(x)$ is a nontrivial factorization of $p(x)$ in $F[x]$, then there exists $t \in F^{\times}$ such that $tA(x) \in R[x]$ and $t^{-1}B(x) \in R[x]$

Corollary. *Suppose $f(x) \in \mathbb{Z}[x], \deg(f(x)) \geq 1$, and $f(x)$ is irreducible in $\mathbb{Z}[x]$. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$*

Definition 2.25. primitive
Suppose R is an integral domain and $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. We say that $f(x)$ is **primitive** in $R[x]$ if its coefficients $a_0, a_1, \ldots, a_n$ are relatively prime in R.

Corollary. *Suppose R is a UFD and F is its field of fractions. Let $f(x) \in R[x]$ with $\deg(f) \geq 1$. The following are equivalent:*

1. *$f(x)$ is irreducible in $R[x]$*
2. *$f(x)$ is primitive in $R[x]$ and irreducible in $F[x]$*

Corollary. *Suppose R is a UFD. Every nonzero polynomial $f(x) \in R[x]$ can be factored $f(x) = dg(x)$ were $d \in R$, $g(x) \in R[x]$, and $g(x)$ is primitive*

Lemma. *Suppose R is a UFD, $c, d \in R$ are non zero, and $f(x), g(x) \in R[x]$ are primitive. If $(cf) \subset (dg)$ then*

1. *$(c) \subseteq (d)$*
2. *$\deg(f) \geq \deg(g)$*
3. *Either $(c) \subset (d)$ or $\deg(f) > \deg(g)$*

Theorem 2.6. *If R is a UFD, then so is $R[x]$*

Corollary. *If R is a UFD, then the ring $R[x, y]$ of polynomials over R in two variables is a UFD.*