Basic Group Theory and Ring Theory

Yunhai Xiang

August 5, 2019

Contents

1 Groups and Subgroups 2

2 Cyclic Groups and Quotient Groups 2

3 Normal Subgroups 2

4 Isomorphisms and Homomorphisms 2

5 Group Actions 2

6 Fundamental Theory of Abelian Groups 2

7 Rings 2

8 Rings and Ideals 3

1 Groups and Subgroups

2 Cyclic Groups and Quotient Groups

3 Normal Subgroups

4 Isomorphisms and Homomorphisms

5 Group Actions

6 Fundamental Theory of Abelian Groups

7 Rings

Definition 7.1. A **ring** is a group R under the operation $+ : R \times R \to R$ (which we call the addition) and with an additional operation $\cdot : R \times R \to R$ (which we call the multiplication) such that for $a, b, c \in R$,

1. $(ab)c = a(bc)$, and
2. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$

Note that we denote $a \cdot b$ as ab, and $a + (-b)$ as $a - b$. If a ring R is such that there exists $1 \in R$ such that $1a = a1 = a$ for all $a \in R$ then R is said to be **unital**. If a ring R is such that $ab = ba$ for all $a, b \in R$, then R is said to be **communtative**.

Definition 7.2. Let R be a unital ring, and let $a \in R$ be nonzero. If there exists $b \in R$ such that $ab = 1$ then we say that b is the **inverse** of a and a is a **unit** or a is **invertible**, and we write $b = a^{-1}$. If there exists nonzero $b \in R$ such that $ab = 0$ then a is said to be a **zero divisor**.

Proposition 7.3 (Facts about units and zero divisors)**.** Let R be a unital ring, then

1. $1 \in R$ is unique,
2. for a unit $a \in R$, a^{-1} is unique,
3. for a unit $a \in R$, $(a^{-1})^{-1} = a$,
4. a zero divisor is not a unit and a unit is not a zero divisor.

Definition 7.4. If R is a ring and $S \subseteq R$ is also a ring under the same operations then we say S is a **subring** of R.

8 Rings and Ideals

Definition 8.1. Let R be a unital ring, we define the **characteristic** of R as the least positive integer n such that the sum of n numbers of 1 is 0,

$$\operatorname{char} R = \min\{n \in \mathbf{Z}^+ \mid \underbrace{1 + 1 + \cdots + 1}_{n} = 0\}$$

and if such positive integer does not exist, we say that the characteristic is infinite, and we write $\operatorname{char} R = \infty$.

Proposition 8.2. If R is an integral domain then $\operatorname{char} R = 0$ or $\operatorname{char} R = p$ for some prime p.

Proof. Suppose the converse that $\operatorname{char} R = ab$ for some integers $1 < a, b < n$, since $n = \operatorname{char} R$ is the least positive integer such that $\sum_{i=1}^{n} 1 = 0$, we have $\sum_{i=1}^{a} 1 \neq 0$ and $\sum_{j=1}^{b} 1 \neq 0$, since R is an integeral domain,

$$0 \neq \left(\sum_{i=1}^{a} 1\right)\left(\sum_{j=1}^{b} 1\right) = \sum_{i=1}^{a}\sum_{j=1}^{b} 1 = \sum_{i=1}^{\operatorname{char} R} 1 = 0$$

a contradiction. □

Definition 8.3. Let R be a ring, $S \subseteq R$ is a **subring** of R if S is also a ring under the same operations as R. If S is a subring of R and $S \neq R$ then we say S is a **proper subring**.

Proposition 8.4. (Subring Test) Let R be a ring and $S \subseteq R$ a nonempty subset, then S is a subring iff

1. $a, b \in S$ implies $a - b \in S$, and
2. $a, b \in S$ implies $ab \in S$.

Definition 8.5. Let R be a ring and I a subring of R, then I is an **ideal** if $a \in I$, $r \in R$ implies $ar, ra \in I$. If I is an ideal of R and $I \neq R$ then we say I is a **proper ideal**.

Proposition 8.6. The only ideals of a field F are $\{0\}$ and F.

Definition 8.7. Let R be a communtative and unital ring then an ideal I of R is a **principle** ideal if there exists $x \in R$ such that $I = \langle x \rangle$, where

$$\langle x \rangle = \{rx \mid r \in R\}$$

and we say that x is the **generator** of the ideal I. Moreover, an integral domain R is called a **principle ideal domain** if all of its ideals are principle ideals.