1 – REVIEW OF RING THEORY

Colin Commans

Definitions

We first recall familiar definitions.

Definition. A **ring** is a nonempty set R, together with two binary operations addition $(+)$ and multiplication $(\cdot)$ where:

1. R is an abelian group under addition:
   - $\forall a, b, c \in R$, $(a+b)+c = a+(b+c)$
   - $\exists\ 0 \in R$ such that $\forall a \in R$, $0 + a = a + 0 = a$
   - $\forall a \in R$, $\exists\ -a \in R$ such that $a + (-a) = -a + a = 0$
   - $\forall a, b \in R$, $a + b = b + a$
2. Multiplication is associative: $\forall a, b, c \in R$, $(ab)c = a(bc)$
3. Multiplicative identity: $\exists\ 1\ (1 \neq 0)$ such that $a1 = 1a = a$ for any $a \in R$
4. Distributivity: $\forall a, b, c \in R$, $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$

R is a **commutative ring** if multiplication is commutative, i.e. $ab = ba$ for any $a, b \in R$.

Definition. Let R be a ring. $a \in R$ is a **unit** or **invertible** if it has a multiplicative inverse, i.e. $\exists\ a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$. The set of all units in R is denoted $R^\times$ or R^*.

Definition. A nonzero commutative ring R is called an **integral domain** if R has no zero divisors, i.e. for any $a, b \in R$,

$$ab = 0 \implies a = 0 \text{ or } b = 0$$

Fields

Definition. A nonzero commutative ring R is a **field** if every nonzero element of R has an inverse (or $R \setminus \{0\}$ is an abelian group under $\cdot$).

[**N.B.** Arbitrary fields will be denoted $E, F, K, L, \ldots$.]

Therefore in a field, multiplication is almost as strong as addition, but 0 has no multiplicative inverse, so the two operations are not symmetric. We thus have the interesting properties:

1. A field only has two ideals: 0 and the field itself. Hence the notion of a quotient field is essentially meaningless. Also, every nonzero ring homomorphism between fields in injective (we will call such maps **embeddings** later).
2. The Cartesian product of fields is not a field, since
$$(0, 1) \cdot (1, 0) = (0, 0)$$
i.e. zero divisors exist.
3. If $F \leq E$ is a **field extension**, i.e. F is a subfield of E, then we can view E as a vector space over F.

Remark.
Note that any field must necessarily be an integral domain, since if $ab = 0$ and if $a \neq 0$, then a^{-1} exists and

$$0 = a^{-1}0 = a^{-1}ab = b$$

Thus either $b = 0$ or $a = 0$. △

Theorem.

1. *A finite integral domain is a field.*

2. *The ring $\mathbb{Z}_n$ is a field if and only if n is prime.*

Proof.

1. Let R be a finite integral domain. We only need to show that all nonzero elements are invertible. Choose $a \in R$ such that $a \neq 0$ and $a \neq 1$. We know that

$$\langle a \rangle = \{a^n \mid n = 1, 2, \dots\}$$

is a (multiplicative) subgroup of R, hence it is finite. In particular, $1 \in \langle a \rangle$, so $1 = a^m$ for some $m > 1$. Now setting $b = a^{m-1}$, we have

$$1 = a^m = \begin{cases} a^{m-1}a = ba \\ aa^{m-1} = ab \end{cases}$$

Thus a is invertible.

2. $\Longleftarrow$: Let n be prime. $\mathbb{Z}_n$ is a nonzero commutative ring, so we only need to show multiplicative inverses exist. Choose $a \in \mathbb{Z}_n$ with $a \neq 0$. Since $0 < a < n$, we have a not a multiple of n. Since n is prime, this means $\gcd(a, n) = 1$. By Bezout's identity, there exists $p, q \in \mathbb{Z}$ such that $pa + qn = 1$. Now if we set $p' \equiv p \mod n$, we have

$$pa + qn = 1 \implies p'a + 0 \equiv 1 \mod n \implies p' = a^{-1}$$

$\Longrightarrow$: Let n be not prime. Then we can write $n = ab$ for $1 < a, b < n$. In particular, a and b are nonzero but

$$ab \equiv 0 \in \mathbb{Z}_n$$

Hence $\mathbb{Z}_n$ is not an integral domain, which from the remark means $\mathbb{Z}_n$ is not a field.

□

Definition. Let R be a ring. The smallest possible integer c for which

$$c1 := \underbrace{1 + 1 + \cdots + 1}_{c} = 0$$

or equivalently for which $cR = \{0\}$, is called the **characteristic** of R, denoted $c = \mathrm{char}(R)$. If no such number exists, we say that R has characteristic zero.

Theorem.
All fields have prime characteristic, or characteristic zero.

Proof.
Let F be a field and let $c = \mathrm{char}(F) \neq 0$. Now suppose $c = ab$. Then

$$\begin{aligned}
0 = c1 = (ab)1 &= \underbrace{1 + 1 + \cdots + 1 + 1 + 1 + \cdots + 1}_{ab} \\
&= \underbrace{\underbrace{(1 + 1 + \cdots + 1)}_{a} + \cdots + \underbrace{(1 + 1 + \cdots + 1)}_{a}}_{b \text{ times}} \\
&= \underbrace{(1 + 1 + \cdots + 1)}_{a} \cdot \underbrace{(1 + 1 + \cdots + 1)}_{b} && \text{(via Distributivity)} \\
&= a1 \cdot b1
\end{aligned}$$

Now, note that F must be an integral domain, so either $a1 = 0$ or $b1 = 0$. But since by definition c is the smallest such integer, therefore $a = c$ or $b = c$. Thus c is irreducible, hence prime. $\square$

Theorem.
If F is a field and S is a finite subgroup of the multiplicative group $F^\times$, then S is a cyclic group. In particular, if F is finite then $F^\times$ is cyclic.

Proof.
We want to find a single generator of S, i.e. find $x \in S$ such that $S = \langle x \rangle$. Equivalently,

$$S = \langle x \rangle \iff x^{|S|} = 1 \iff \mathrm{ord}(x) = |S|$$

Assume otherwise, i.e. the largest order of an element of S is some number $n < |S|$. This means that n divides the order of every element of S, i.e. n is the lcm of all orders. Therefore for every $x \in S$, we have $x^n = 1$. However, the polynomial

$$x^n - 1$$

can only have at most n roots in F (and thus in S) as F is a field. Therefore

$$|S| = |\{x \in S \mid x^n - 1 = 0\}| \leq n < |S|$$

which is a contradiction. $\square$