10. Basic properties of rings

Lemma 10.1. *Let R be a ring and let a and b be elements of R. Then*

(1) $a0 = 0a = 0$.
(2) $a(-b) = (-a)b = -(ab)$
(3) $(-a)(-b) = ab$.

Proof. Let $x = a0$. We have

$$\begin{aligned} x &= a0 \\ &= a(0+0) \\ &= a0 + a0 \\ &= x + x. \end{aligned}$$

Adding $-x$ to both sides, we get $x = 0$. By symmetry $0a = 0$. This is (1).

Let $y = a(-b)$. We want to show that y is the additive inverse of ab, that is, we want to show that $y + ab = 0$. We have

$$\begin{aligned} y + ab &= a(-b) + ab \\ &= a(-b+b) \\ &= a0 \\ &= 0, \end{aligned}$$

by (1). By symmetry $(-a)b = -ab$. Hence (2).

$$\begin{aligned} (-a)(-b) &= -(a(-b)) \\ &= - - ab \\ &= ab, \end{aligned}$$

which is (3). $\square$

Definition 10.2. *Let $\phi\colon R \longrightarrow S$ be a function between two rings. We say that ϕ is a* ***ring homomorphism*** *if for every a and $b \in R$,*

$$\begin{aligned} \phi(a+b) &= \phi(a) + \phi(b) \\ \phi(a \cdot b) &= \phi(a) \cdot \phi(b). \end{aligned}$$

Note that a ring homomorphism is automatically a group homomorphism. In particular the kernel of ϕ is an additive subgroup of R and ϕ is one to one if and only if $\operatorname{Ker}\phi = \{0\}$.

Example 10.3. *Let F be the ring of all functions from $\mathbb{R}$ to $\mathbb{R}$. Given $a \in \mathbb{R}$ we have an* ***evaluation homomorphism***

$$\phi_a\colon F \longrightarrow \mathbb{R} \qquad \text{given by} \qquad f \longrightarrow f(a),$$

which sends a function $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ to its value at a.

We have already seen that ϕ is a group homomorphism. We check it is a ring homomorphism. Pick f and $g \in F$. Then

$$\begin{aligned}\phi(fg) &= (fg)(a)\\ &= f(a)g(a)\\ &= \phi(f)\phi(g).\end{aligned}$$

Therefore ϕ is a ring homomorphism.

Example 10.4. *Let $\phi\colon \mathbb{Z} \longrightarrow \mathbb{Z}_n$ be the map which sends a to its remainder r modulo n.*

We have already seen that ϕ is a group homomorphism. We check it is a ring homomorphism. Suppose that a and b are integers. We may write

$$a = q_1 n + r_1 \qquad \text{and} \qquad b = q_2 n + r_2.$$

Then

$$\begin{aligned}ab &= (q_1 n + r_1)(q_2 n + r_2)\\ &= (q_1 q_2 n + r_1 q_2 + r_2 q_1)n + r_1 r_2.\end{aligned}$$

It follows that

$$\begin{aligned}\phi(ab) &= r_1 r_2\\ &= \phi(a)\phi(b).\end{aligned}$$

Definition 10.5. *A ring homomorphism $\phi\colon R \longrightarrow R'$ is an* ***isomorphism*** *if ϕ is one to one and onto.*

Example 10.6. *Consider the two rings $\mathbb{Z}$ and $2\mathbb{Z}$.*

These are isomorphic as groups, since the function

$$\mathbb{Z} \longrightarrow 2\mathbb{Z} \qquad \text{which sends} \qquad n \longrightarrow 2n,$$

is a group homomorphism is one to one and onto. However ϕ is not an isomorphism of rings (in fact they are not isomorphic as rings). Indeed,

$$\phi(1.1) = \phi(1) = 2 \qquad \text{whilst} \qquad \phi(1)\phi(1) = 2 \cdot 2 = 4 \neq 2.$$

Thus

$$\phi(1.1) \neq \phi(1)\phi(1).$$

Definition 10.7. *We say that the ring R is* ***commutative*** *if multiplication is commutative.*

(8) *(Commutativity)* $a \cdot b = b \cdot a$.

We say that R is a ***ring with unity*** *if*

(9) *(Unity) There is an element $1 \in R$ such that for all a in R,*

$$a \cdot 1 = a = 1 \cdot a.$$

Note that matrix groups $M_n(R)$ are not commutative in general, even when R is commutative but if R has unity $M_n(R)$ does have unity, since the identity matrix acts as the identity. The integers, rationals, reals and complex numbers are commutative rings with unity. However $2\mathbb{Z}$ is a commutative ring without unity. In particular it is not isomorphic to the integers.

Let R be the ring with a single element 0. Then R is a commutative ring with unity. In all other rings, $1 \neq 0$.

Example 10.8. *Let R and S be two rings. Then $R \times S$ is commutative if and only if R and S are commutative and $R \times S$ is a ring with unity if and only if R and S are rings with unity.*

Definition 10.9. *Let R be a ring with unity, $1 \neq 0$.*

An element $u \in R$ is called a ***unit*** *if u has a multiplicative inverse in R, that is, there is an element $v \in R$ such that $uv = 1 = vu$.*

We say that R is a ***division ring*** *if every non-zero element of R is a unit. We say that R is a* ***field*** *if R is a commutative division ring.*

Note that zero is never a unit in a ring with unity $1 \neq 0$. Indeed,

$$0a = 0 \neq 1.$$

Example 10.10. *What are the units in $\mathbb{Z}_{15}$?*

Note that the multiples of 3:

$$3, \qquad 6, \qquad 9, \qquad \text{and} \qquad 12$$

are not units, since a multiple, of a multiple of three, is a multiple of three:

$$m(3n) = 3mn,$$

and the remainder when you divide by 15 is still a multiple of three.

Similarly the multiples of 5:

$$5 \qquad \text{and} \qquad 10$$

are also not units.

1, and $14 = -1$ are units, since

$$14 \cdot 14 = (-1)(-1) = 1.$$

2 is a unit, since

$$2 \cdot 8 = 16 = 1 \mod 15.$$

By the same token, 8 is a unit and so both

$$13 = -2 \qquad \text{and} \qquad 7 = -8 \mod 15.$$

are units, since

$$13 \cdot 7 = (-2) \cdot (-8) = 2 \cdot 8 = 1 \mod 15.$$

4 is a unit, since

$$4^2 = 16 = 1 \mod 15.$$

Therefore $11 = -4 \mod 15$ is also a unit, as

$$11^2 = (-4)^2 = 4^2 = 1 \mod 15.$$

Thus the units are

$$1, \qquad 2, \qquad 4, \qquad 7, \qquad 8, \qquad 11, \qquad 13, \qquad \text{and} \qquad 14.$$

Example 10.11. *The only units in $\mathbb{Z}$ are ± 1; $\mathbb{Z}$ is not a field. For example 2 does not have a multiplicative inverse. On the other hand,*

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

is a tower of subfields.

Let us introduce some convenient notation. If $a \in R$ then

$$a + a = 2 \cdot a \qquad a + a + a = 3 \cdot a \qquad \text{and} \qquad a + a + \cdots + a = n \cdot a.$$

Note that this is not the same as multiplication in the ring, it is just very convenient shorthand; for example most rings won't contain 2 or 3.

Lemma 10.12. *If r and s are coprime natural numbers then the rings $\mathbb{Z}_{rs}$ and $\mathbb{Z}_r \times \mathbb{Z}_s$ are isomorphic.*

Proof. The two additive groups $\mathbb{Z}_{rs}$ and $\mathbb{Z}_r \times \mathbb{Z}_s$ are isomorphic as groups, since they are both cyclic groups of order rs. As 1 is a generator of $\mathbb{Z}_{rs}$ and $(1, 1)$ is a generator of $\mathbb{Z}_r \times \mathbb{Z}_s$, if we define a map

$$\phi \colon \mathbb{Z}_{rs} \longrightarrow \mathbb{Z}_r \times \mathbb{Z}_s \qquad \text{by the rule} \qquad n = n \cdot 1 \longrightarrow n \cdot (1, 1),$$

then ϕ is an isomorphism of groups. To check it is a ring homomorphism, observe that

$$\begin{aligned} \phi(nm) &= (nm) \cdot (1, 1) \\ &= [n \cdot (1, 1)][m \cdot (1, 1)] \\ &= \phi(n)\phi(m). \end{aligned}$$

Thus ϕ is a ring homomorphism and so ϕ is a ring isomorphism. $\square$