IDEALS OF A COMMUTATIVE RING

1. Rings

Recall that a **ring** $(R, +, \cdot)$ is a set R endowed with two binary operations such that $(R, +)$ is an abelian group, and such that for all $r, s, t \in R$,

$$r(st) = (rs)t,$$
$$r(s + t) = rs + rt,$$
$$(r + s)t = rt + st.$$

Multiplication need not commute, and the ring need not contain a multiplicative identity. (For example, the linear endomorphisms of a vector space V over a field k form a noncommutative ring $\mathrm{End}_k(V)$, and if V has finite dimension n then the ring can identified—noncanonically—with the matrix ring $\mathrm{M}_n(k)$. And for example, the even integers form a commutative ring $2\mathbb{Z}$ that has no multiplicative identity.) When the ring operations are clearly understood, we write R rather than $(R, +, \cdot)$.

In any ring, the additive identity is a multiplicative annihilator. Indeed, for any ring element r we have

$$0_R r = (0_R + 0_R)r = 0_R r + 0_R r,$$

so that adding the additive inverse of $0_R r$ to both sides gives

$$0_R r = 0_R, \quad r \in R.$$

And similarly $r0_R = 0_R$ for all $r \in R$.

Let R and $\widetilde{R}$ be rings. A **ring homomorphism** between them is a map

$$f : R \longrightarrow \widetilde{R}$$

such that for all $r, s \in R$,

$$f(r + s) = f(r) + f(s),$$
$$f(rs) = f(r)f(s).$$

That is, f is an abelian group homomorphism that also preserves multiplication. As always, the operations on the left side of the equalities in the homomorphism rules are set in R while the operations on the right side are set in $\widetilde{R}$.

Let $f : R \longrightarrow \widetilde{R}$ be a ring homomorphism, and let I be its kernel. Then I is a subgroup of R as an abelian group (in fact I is a normal subgroup of R, but in the abelian group all subgroups are normal and so the normality deserves no mention). But also, for any $i \in I$ and any $r \in R$ we have

$$f(ri) = f(r)f(i) = f(r)0_{\widetilde{R}} = 0_{\widetilde{R}},$$

and similarly $f(ir) = 0_{\widetilde{R}}$. That is:

> *The kernel of any ring homomorphism is not only an additive subgroup of the domain ring, it is also strongly closed under multiplication from both sides.*

Thus a kernel is a subring, but it has even stronger closure properties than a general subring. The phenomenon is in close analogy to how any kernel of a group homomorphism is not only a subgroup of the domain group but is in fact a normal subgroup. By analogy to groups, we suspect that

- The quotient space of a ring by a kernel again has the structure of a ring.
- Any subring with the stronger closure properties allows the formation of such a quotient and is a kernel.
- (First Ring Isomorphism Theorem) If $f : R \longrightarrow \widetilde{R}$ is a ring homomorphism then it induces a natural isomorphism

$$\tilde{f} : R/\ker(f) \xrightarrow{\sim} \mathrm{im}(f), \quad r + \ker(f) \longmapsto f(r).$$

Indeed all three suppositions are correct, as we will see.

2. Ideals and Quotients

Again let R be a ring. Let $I \subset R$ be a subring.

The resulting *set* of I-cosets,

$$R/I = \{r + I : r \in R\},$$

is perfectly sensible, and the only natural ring operations for R/I could be those inherited from R,

$$\begin{aligned}(r + I) + (s + I) &= r + s + I,\\ (r + I)(s + I) &= rs + I.\end{aligned}$$

Granting these operations, the ring axioms for R/I will follow from the ring axioms for R. For example, the calculation

$$\begin{aligned}\big((r + I)(s + I)\big)(t + I) &= (rs + I)(t + I)\\ &= (rs)t + I\\ &= r(st) + I\\ &= (r + I)(st + I)\\ &= (r + I)\big((s + I)(t + I)\big)\end{aligned}$$

shows that associativity is inherited. But as always:

The question is whether the operations are **well-defined**.

Since the ring R is an abelian group under addition, the subring I is a normal subgroup under addition, and so the addition operation on the quotient space poses no problem. But the multiplication operation requires more scrutiny. Compute that

$$(r + I)(s + I) = rs + rI + Is + II.$$

Since I is a subring we have $II \subset I$. (But they may not be equal, since the subring I need not contain 1; indeed, even the full ring need not contain a multiplicative identity.) So in fact we have

$$(r + I)(s + I) \subset rs + rI + Is + I.$$

But now, in order to continue, we must assume that the subring I is in fact *strongly* closed under multiplication,

$$rI \subset I \text{ and } Ir \subset I \quad \text{for all } r \in R.$$

Such a subring has its own name:

Definition 2.1 (Ideal)**.** *Let R be a ring. An additive subgroup I of R that is also strongly closed under multiplication is called an* **ideal** *of R.*

Granting that the subring I is an ideal, we now have

$$(r+I)(s+I) \subset rs+I.$$

That is:

> *If the subring I of R is an ideal then the* **set** $(r+I)(s+I)$ *is a* **subset** *of the coset $rs+I$. Thus we should define the* **coset product** $(r+I)(s+I)$ *to be the* **full** *coset $rs+I$.*

Contrast this with the situation for groups. If G is a group and N is a normal subgroup then the relation

$$gN \cdot g'N = gg'N \qquad \text{(equality of subsets of } G\text{)}$$

must also be the formula for coset multiplication,

$$gN \cdot g'N = gg'N \qquad \text{(product of cosets in } G/N\text{)},$$

but if R is a ring and I is an ideal then we have only

$$(r+I)(s+I) \subset rs+I \quad \text{(containment of subsets of } R\text{)},$$

but still the containment forces the rule

$$(r+I)(s+I) = rs+I \quad \text{(product of cosets in } R/I\text{)}.$$

Although we have deduced that the coset multiplication rule for R/I has a chance to be well-defined only if I is an ideal, we haven't yet shown that if I is an ideal then the coset multiplication rule really *is* well-defined. What needs to be shown is that

$$\left\{\begin{array}{l} r+I=\rho+I \\ s+I=\sigma+I \end{array}\right\} \implies rs+I=\rho\sigma+I.$$

Equivalently, what needs to be shown is that

$$\left\{\begin{array}{l} \rho-r\in I \\ \sigma-s\in I \end{array}\right\} \implies \rho\sigma-rs\in I.$$

But indeed,

$$\rho\sigma-rs=\rho\sigma-r\sigma+r\sigma-rs=(\rho-r)\sigma+r(\sigma-s),$$

and the right side of the display lies in I since $\rho-r$ and $\sigma-s$ do and since I is an ideal. Note how the argument requires that I be strongly closed under multiplication from both sides.

To summarize the discussion: Let R be a commutative ring, and let $I \subset R$ be an ideal. Then the quotient space of I-cosets in R,

$$R/I = \{r+I : r\in R\},$$

is again a ring under the natural definitions of addition and multiplication,

$$\begin{aligned} (r+I)+(s+I) &= r+s+I, \\ (r+I)(s+I) &= rs+I. \end{aligned}$$

The ring R/I is called the **quotient ring** of R by I. And I is the kernel of the natural projection map

$$R \longrightarrow R/I, \quad r \longmapsto r + I.$$

So indeed every ideal is a kernel, just as every kernel is an ideal.

The first isomorphism theorem for rings is proved exactly as it is proved for groups.

3. Maximal Ideals and Prime Ideals

Definition 3.1 (Maximal Ideal, Prime Ideal)**.** *Let R be a ring. Then:*

- *An ideal I of R is* **maximal** *if the only ideal of R properly containing I is R itself.*
- *An ideal I of R is* **prime** *if*

$$\text{for all } r, s \in R, \quad rs \in I \implies r \in I \text{ or } s \in I.$$

Now we add the hypothesis that R is a *commutative* ring *with multiplicative identity*. That is, $rs = sr$ for all $r, s \in R$, and R contains an element 1 such that $1r = r$ for all $r \in R$. Note that now an ideal of R is all of R if and only if contains 1.

Let I be an ideal of R. The condition that

$$I \text{ is maximal}$$

is equivalent to the condition (letting the symbol r denote a ring element)

$$\text{for all } r \notin I, \quad \text{the ideal } \langle r, I \rangle \text{ is all of } R,$$

which in turn is equivalent to

$$\text{for all } r \notin I, \quad rs + i = 1 \text{ for some } s \in R \text{ and } i \in I,$$

or,

$$\text{for all } r \notin I, \quad rs + I = 1 + I \text{ for some } s \in R,$$

or,

$$\text{for all nonzero } r + I \in R/I, \quad (r + I)(s + I) = 1 + I \text{ for some } s + I \in R/I,$$

or,

$$R/I \text{ is a field.}$$

Similarly, the condition

$$I \text{ is prime}$$

is equivalent to the condition (letting the symbols r, s denote ring elements)

$$\text{for all } r, s \notin I, \quad \text{also } rs \notin I,$$

which in turn is equivalent to

$$\text{for all nonzero } r + I, s + I \in R/I, \quad \text{also } (r + I)(s + I) \text{ is nonzero in } R/I,$$

or, recalling that a commutative ring with multiplicative identity is an *integral domain* if it contains no zero-divisors,

$$R/I \text{ is an integral domain.}$$

Since every field is an integral domain but not necessarily conversely, we have proved the following result.

Proposition 3.2. *Let R be a commutative ring with multiplicative identity. Let I be an ideal of R. Then*

- *The ideal I is maximal if and only if the quotient ring R/I is a field.*
- *The ideal I is prime if and only if the quotient ring R/I is an integral domain.*
- *If the ideal I is maximal then it is prime, but not necessarily conversely.*

A slightly tricky feature of the language is that

- At the level of ring *elements*, prime and not zero-divisor implies irreducible.
- But at the level of ring *ideals*, maximal implies prime.

The issue is that although ideals can be multiplied, the multiplication of ideals closely reflects the multiplication of ring elements only when the ideals are *principal*. Here are some examples to illustrate how the definitions interplay.

(1) *In a principal ideal domain, if an element r is irreducible then the ideal (r) is maximal.* Indeed, if r generates a non-maximal ideal then there exist proper containments $(r) \subset (s) \subset R$. Thus $r = st$ where neither s nor t is associate to 1. That is, r is not irreducible. The result follow by contraposition.
(2) However, in the non-PID $R = \mathbb{Z}[X]$, consider a rational prime $p \in \mathbb{Z}$. Then p is irreducible in R, but the ideal (p) is not maximal because the ideal $I = \langle p, X \rangle$ properly contains it without being all of R.
(3) *No longer assuming a PID, if (r) is maximal and r does not divide 0 then r is irreducible.* Indeed, if (r) is maximal then by the second bullet (r) is prime, and so, since multiplication of principal ideals mirrors multiplication of ring elements up to units (multiplicatively invertible elements, which we don't care about anyway), r is prime. If also r does not divide 0 then the first bullet says that r is irreducible.
(4) However, in the ring $\mathbb{Z}/6\mathbb{Z}$, the element $r = 3 + 6\mathbb{Z}$ of the ring $R = \mathbb{Z}/6\mathbb{Z}$ generates a maximal ideal but is not irreducible since $r = r^2$. The issue is that r is a zero-divisor.

4. The Quotient Field of an Integral Domain

Let R be an integral domain. Its **quotient field** is defined as follows. Consider the set of ordered pairs from R whose second entry is nonzero,

$$\{(r, s) : r, s \in R,\ s \neq 0\}.$$

Define an equivalence relation on the set,

$$(r, s) \sim (r', s') \quad \text{if} \quad rs' = r's.$$

Then the quotient field is the set of equivalence classes,

$$\mathrm{QF}(R) = \{(r, s) : r, s \in R,\ s \neq 0\}/\sim,$$

endowed with the operations (using square brackets to denote equivalence classes)

$$[r, s] + [r', s'] = [rs' + r's, ss'],$$
$$[r, s][r', s'] = [rr', ss'].$$

Purely formal verifications show that the operations are well-defined, that $\mathrm{QF}(R)$ is a field, and that the map

$$R \longrightarrow \mathrm{QF}(R), \quad r \longmapsto [r, 1]$$

is a monomorphism of rings. The process is exactly the same as constructing the field of rational numbers from the ring of integers and checking that the construction

is sensible. The usual notation for $[r, s]$ is r/s, and the equivalence relation simply encodes the usual cancellation rule for fractions.

5. Localization

Again let R be an integral domain. Let P be a prime ideal of R. The **localization** of R at P is a subring of the quotient field $\mathrm{QF}(R)$,

$$R_{(P)} = \{[r, s] : r \in R,\ s \notin P\}.$$

The point is that (using the usual informal notation) if r/s and r'/s' have denominators not in P then so do $r/s + r'/s'$ and $r/s \cdot r'/s'$.

For example, localizing the basic integer ring $\mathbb{Z}$ at a prime ideal $p\mathbb{Z}$ gives the ring $\mathbb{Z}_{(p\mathbb{Z})}$ of rational numbers with denominators not divisible by p. The ideal structure of the localized ring is very simple,

$$\mathbb{Z}_{(p\mathbb{Z})} \supset p\mathbb{Z}_{(p\mathbb{Z})} \supset p^2\mathbb{Z}_{(p\mathbb{Z})} \supset \cdots .$$

Similarly, localizing the polynomial ring $k[X]$ (where X is a field) at a prime ideal $(X-a)k[X]$ gives the ring $k[X]_{((X-a)k[X])}$ of rational functions whose denominators are not divisible by $X - a$. Again the ideal structure is simple,

$$k[X]_{((X-a)k[X])} \supset ((X-a)k[X])_{((X-a)k[X])} \supset (X-a)^2k[X]_{((X-a)k[X])} \supset \cdots .$$