Ideals

The symbol R always denotes a commutative ring with unity, and F always denotes a field.

1 Definitions and examples

We begin by discussing the following question: let R be a ring and let H be an additive subgroup of $(R, +)$. We can then form the group of cosets $R/H = \{r + H : r \in R\}$ of H. By analogy with the case of $R = \mathbb{Z}$ and $H = \langle n \rangle = n\mathbb{Z}$, where we know that it is possible both to add and to multiply cosets, we want to find conditions on H so that coset multiplication is well-defined, i.e. independent of the choice of representative. Here, as in the case of $\mathbb{Z}/n\mathbb{Z}$, we attempt to define coset multiplication by the rule: $(r + H)(s + H) = rs + H$. In particular, this is well defined $\iff$ for all $r, s \in R$, replacing r by a different representative $r + h_1$ of $r + H$ and s by a different representative $s + h_2$ of $s + H$, the product $(r + h_1)(s + h_2)$ lies in $rs + H$. In other words, for all $r, s \in R$ and $h_1, h_2 \in H$, there exists an $h_3 \in H$ such that $(r + h_1)(s + h_2) = rs + h_3$. Since $(r + h_1)(s + h_2) = rs + rh_2 + sh_1 + h_1h_2$, another way to say this is: for all $r, s \in R$ and $h_1, h_2 \in H$,

$$rh_2 + sh_1 + h_1h_2 \in H.$$

In particular, taking $h_2 = h$ an arbitrary element of H and $s = h_1 = 0$,

$$rh_2 + sh_1 + h_1h_2 = rh + 0 + 0.$$

Thus we see that a necessary condition that coset multiplication is well-defined is that, for all $r \in R$ and $h \in H$, the product $rh \in H$. Conversely, if this condition is satisfied, then, for all $r, s \in R$ and $h_1, h_2 \in H$, $rh_2 \in H$, $sh_1 \in H$, and $h_1h_2 \in H$ (take $r = h_1$ and $h = h_2$). Hence, as H is closed under addition, coset multiplication is well-defined.

Definition 1.1. A subset I of R is an *ideal* if

1. I is an additive subgroup of $(R, +)$;

2. (The "absorbing property") For all $r \in R$ and $s \in I$, $rs \in I$; symbolically, we write this as $RI \subseteq I$.

For example, for all $d \in \mathbb{Z}$, the cyclic subgroup $\langle d \rangle$ generated by d is an ideal in $\mathbb{Z}$. A similar statement holds for the cyclic subgroup $\langle d \rangle$ generated by d in $\mathbb{Z}/n\mathbb{Z}$. However, for a general ring R and an element $r \in R$, the cyclic subgroup $\langle r \rangle = \{n \cdot r : n \in \mathbb{Z}\}$ is almost never an ideal. We shall describe the correct generalization of $\langle r \rangle$ to an arbitrary ring shortly.

Remark 1.2. It is easy to see that I is an ideal of $R \iff I$ is nonempty, closed under addition, and the absorbing property $RI \subseteq I$ holds. The $\implies$ direction is clear since an additive subgroup of R is nonempty and closed under addition. To show the $\impliedby$ direction, it is enough to show that I is an additive subgroup, and hence it suffices to show that $0 \in I$ and that, for all $s \in I$, $-s \in I$. To see that $0 \in I$, note that $I \neq \emptyset$ by assumption, hence there exists some $s \in I$. Then $0 = 0s \in I$. Also, if $s \in I$, $-s = (-1)s \in I$. Thus I is an additive subgroup.

Summarizing the discussion before the definition of an ideal, we have:

Proposition 1.3. *Suppose that I is an ideal. Then coset multiplication is well-defined on R/I. Moreover, $(R/I, +, \cdot)$ is a ring, called the quotient ring, and the function $\pi \colon R \to R/I$ defined by $\pi(r) = r + I$ is a ring homomorphism, called the quotient homomorphism.*

Proof. We have seen that coset multiplication is well-defined. It is then easy to check that it is associative and commutative, and that coset multiplication distributes over coset addition: all of these properties follow from properties of multiplication in the ring R. The multiplicative identity in R/I is the coset $1 + I$. Finally, from the definition of coset multiplication, we see that

$$\pi(r)\pi(s) = (r + I)(s + I) = rs + I = \pi(rs).$$

Moreover $\pi(1) = 1 + I$ is the multiplicative identity in R/I. Thus π (which we know from last semester to be a group homomorphism) is a ring homomorphism. $\square$

Remark 1.4. If I is an ideal, we have defined coset multiplication by the formula $(r+I)(s+I) = rs+I$. However, unlike the case of groups, it is not necessarily literally true that, if we define

$$(r + I)(s + I) = \{(r + t_1)(s + t_2) : t_1, t_2 \in I\},$$

then we necessarily have $(r+I)(s+I) = rs+I$ as sets. For example, if $I = \langle n \rangle = n\mathbb{Z}$ in $\mathbb{Z}$, then taking $r = s = 0$, we see that every element t of I is of the form n^2k for some integer k, hence is not the most general element of $0 \cdot 0 + \langle n \rangle = \langle n \rangle$. In general, we can only say that the set $(r+I)(s+I)$ is contained in $rs+I$.

Example 1.5. 1) In any ring R, the set $\{0\}$ is an ideal (the *zero ideal*) and the ring R itself is an ideal (the *unit ideal*). An ideal $I \neq R$ is called *proper ideal*.
2) If R is a ring and I is an ideal of R such that $1 \in I$, then by the absorbing property, for all $r \in R$, $r = r \cdot 1 \in I$, hence $I = R$. More generally, if I is an ideal containing a unit u, then $1 = u^{-1}u \in I$ and hence $I = R$. In particular, if F is a field and I is a nonzero ideal of F, then I contains a unit and hence $I = F$. Thus a field contains no proper nonzero ideals, i.e. every ideal of F is either $\{0\}$ or F.

One way that ideals arise is as follows:

Proposition 1.6. *Let $\phi\colon R \to S$ be a ring homorphism. Then* $\operatorname{Ker}\phi$ *is an ideal in R.*

Proof. We know that $\operatorname{Ker}\phi$ is an additive subgroup of R, so we just have to check the absorbing property. If $r \in \operatorname{Ker}\phi$ and $s \in R$, then $\phi(sr) = \phi(s)\phi(r) = \phi(s) \cdot 0 = 0$. Hence by definition $sr \in \operatorname{Ker}\phi$, so that $\operatorname{Ker}\phi$ has the absorbing property. □

Example 1.7. If R is a ring and $a \in R$, then $\operatorname{Ker}\operatorname{ev}_a = \{f \in R[x] : \operatorname{ev}_a(f) = f(a) = 0\}$ is an ideal in $R[x]$. For example,

$$\operatorname{Ker}\operatorname{ev}_0 = \left\{\sum_{i=0}^{N} a_i x^i : a_0 = 0\right\} = \{xg : g \in R[x]\}.$$

A slightly more complicated argument shows that

$$\operatorname{Ker}\operatorname{ev}_a = \{(x-a)g : g \in R[x]\}.$$

More generally, if R is a subring of a ring S and $b \in S$, then $\operatorname{Ker}\operatorname{ev}_b$ is an ideal in $R[x]$. However, it is usually much more difficult to describe $\operatorname{Ker}\operatorname{ev}_b$.

Remark 1.8. In a non-commutative ring, there are left ideals, right ideals, and two-sided ideals, and for coset multiplication to be well-defined on R/I, we need I to be a two-sided ideal. The analogue of Proposition 1.6 is then that the kernel of a homomorphism is a two sided ideal.

Many of the results about isomorphisms in group theory hold in this context as well. For example, a (ring) homomorphism ϕ is injective $\iff$ $\operatorname{Ker}\phi = 0$, since a ring homomorphism is in particular a homomorphism of abelian groups. Likewise, the first isomorphism theorem holds:

Proposition 1.9. *Let $\phi\colon R \to S$ be a ring homorphism and let $I = \operatorname{Ker}\phi$. The $\operatorname{Im}\phi \cong R/I$. More precisely, there is a unique isomorphism $\tilde{\phi}\colon R/I \to \operatorname{Im}\phi$ such that $\phi = i\circ\tilde{\phi}\circ\pi$, where $\pi\colon R \to R/I$ is the quotient homomorphism and $i\colon \operatorname{Im}\phi \to S$ is the inclusion.*

Proof. The standard argument in group theory shows that, defining $\tilde{\phi}\colon R/I \to \operatorname{Im}\phi$ by $\tilde{\phi}(r+I) = \phi(r)$, $\tilde{\phi}$ is well-defined and is an isomorphism of abelian groups. It then suffices to check that $\tilde{\phi}$ is a ring homomorphism, which follows from the definition of coset multiplication. $\square$

Next we turn to a very general construction of ideals, which is an analogue of the definition of a cyclic subgroup:

Definition 1.10. Let R be a ring and let $r \in R$. The *principal ideal generated by* r, denoted (r), is the set

$$\{sr : s \in R\}.$$

Thus (r) is the set of all multiples of r.

Proposition 1.11. *The principal ideal (r) generated by r is an ideal of R containing r. Moreover, if I is any ideal of R and $r \in I$, then $(r) \subseteq I$.*

Proof. First, (r) is closed under addition: given $s_1r, s_2r \in (r)$, $s_1r + s_2r = (s_1+s_2)r \in (r)$. Moreover $r = 1\cdot r \in (r)$. Hence (r) is nonempty, so to show that it is an ideal it suffices to show that the absorbing property holds. Given $sr \in (r)$ and $t \in R$, $t(sr) = (ts)r \in (r)$. Hence (r) is an ideal of R containing r. Finally, if I is an ideal of R and $r \in I$, then, by the absorbing property, for all $s \in R$, $sr \in I$. Hence $(r) \subseteq I$. $\square$

More generally, if R is a ring and $r_1, \dots, r_n \in R$, the *ideal generated by* $r_1, \dots r_n$ is by definition the ideal

$$(r_1, \dots, r_n) = \left\{\sum_{i=1}^{n} s_ir_i : s_i \in R\right\}.$$

It is an ideal in R, containing $r_1, \dots, r_n$, and is the smallest ideal in R with this property: I is an ideal of R and $r_i \in I$ for all i, then $(r_1, \dots, r_n) \subseteq I$. An ideal of the form $(r_1, \dots, r_n)$ is called a *finitely generated ideal*. For many rings R, such as $F[x_1, \dots, x_n]$, every ideal is finitely generated. But therer are interesting rings such as $C^\infty(\mathbb{R})$ for which some ideals are not finitely generated.

As an application of this construction, we show the following:

Proposition 1.12. *Let R be a ring such that $R \neq \{0\}$. Then R is a field $\iff$ every ideal of R is either $\{0\}$ or R.*

Proof. We have seen the implication $\implies$ in Part 2 of Example 1.5. To see the $\impliedby$ direction, suppose that $R \neq \{0\}$ and that every ideal of R is either $\{0\}$ or R. We must show that, if $r \in R$ and $r \neq 0$, then r is invertible. Consider the principal ideal (r). This is an ideal and it is not equal to $\{0\}$ since $r \in (r)$ and $r \neq 0$. Then by hypothesis $(r) = R$. In particular, $1 \in (r)$. Thus, there exists $s \in R$ such that $sr = 1$. Hence r is a unit. □

2 Prime ideals and maximal ideals

Finally, we want to know when a ring of the form R/I is an integral domain or a field.

Definition 2.1. Let R be a ring. An ideal I in R is a *prime ideal* if $I \neq R$ and, for all $r, s \in R$, if $rs \in I$ then either $r \in I$ or $s \in I$. Equivalently, I is a prime ideal if $I \neq R$ and, for all $r, s \in R$, if $r \notin I$ and $s \notin I$, then $rs \notin I$.

Proposition 2.2. *Let R be a ring and let I be an ideal in R. Then R/I is an integral domain if and only if I is a prime ideal.*

Proof. First note that $I \neq R \iff R/I \neq \{0\}$, so it is enough to show that the condition that for all $r, s \in R$, if $rs \in I$ then either $r \in I$ or $s \in I$ is equivalent to the statement that R/I has no divisors of zero. But R/I has no divisors of zero $\iff$ for all $r, s \in R$ with $r + I \neq 0 = 0 + I$ and $s + I \neq 0 = 0 + I$, the coset product $rs + I \neq 0 + I$. But $r + I \neq 0 = 0 + I$ is equivalent to the statement that $r \notin I$, and similarly for s and rs, so the statement that R/I has no divisors of zero is equivalent to the statement that, if $r \notin I$ and $s \notin I$, then $rs \notin I$. Hence R/I is an integral domain $\iff$ I is a prime ideal. □

Definition 2.3. Let R be a ring. An ideal I in R is a *maximal ideal* if $I \neq R$ and, if J is an ideal in R containing I, then either $J = I$ or $J = R$.

Proposition 2.4. *Let R be a ring and let I be an ideal in R. Then R/I is a field if and only if I is a maximal ideal.*

Proof. As before, $I \neq R \iff R/I \neq \{0\}$, so it is enough to show: for all ideals J containing I, either $J = I$ or $J = R \iff$ every nonzero coset $r + I \in R/I$ has a multiplicative inverse.

$\implies$ Suppose that, for all ideals J containing I, either $J = I$ or $J = R$. Let $r + I$ be a nonzero coset in R/I; equivalently, $r \notin I$. Consider the set

$$J = \{s + tr : s \in I, t \in r\}.$$

Then we claim that J is an ideal of R containing I and r. In fact, J is the ideal sum $I + (r)$ as defined in the homework, and thus is an ideal. To check this directly, note that J is closed under addition since, given $s_1 + t_1r, s_2 + t_2r \in J$,

$$(s_1 + t_1r) + (s_2 + t_2r) = (s_1 + s_2) + (t_1 + t_2)r \in J,$$

and, for all $w \in R$, $s + tr \in J$,

$$w(s + tr) = (ws) + (wt)r \in J.$$

Finally, taking s an arbitrary element of I and $t = 0$, we see that $I \subseteq J$, and taking $s = 0$, $t = 1$, we see that $r \in J$. Thus $J \neq I$, and so $J = R$. In particular, there exist $s \in I$ and $t \in R$ such that $1 = s + tr$. Thus $1 \in (r+I)(t+I)$, so by definition of coset multiplication $(r+I)(t+I) = 1+I$. Hence $r + I$ has a multiplicative inverse.

$\impliedby$: We must show that, if every nonzero coset $r + I \in R/I$ has a multiplicative inverse and J is an ideal of R such that $I \subseteq J$ and $J \neq I$, then $J = R$, or equivalently that $1 \in J$. Since $J \neq I$, there exists $r \in J$, $r \notin I$. Then $r + I$ is not the zero coset, so there exists $s \in I$ such that $(r + I)(s + I) = rs + I = 1 + I$. Equivalently, $rs = 1 + t$, where $t \in I$. Then, since $r \in J$, $rs \in J$, and since $I \subseteq J$, $t \in J$ and hence $rs + t \in J$. Thus $1 \in J$, so that $J = R$. □

Corollary 2.5. *A maximal ideal is a prime ideal.*

Proof. This follows since a field is an integral domain. □

Example 2.6. 1) A ring $R \neq \{0\}$ is an integral domain $\iff$ $(0) = \{0\}$ is a prime ideal. Indeed, in this case R is an an integral domain $\iff$ for all $r, s \in R$, $rs \in (0)$, i.e. $rs = 0$, $\iff$ either $r = 0$ or $s = 0$, i.e. $r \in (0)$ or $s \in (0)$, $\iff$ (0) is a prime ideal. Likewise, by Proposition 1.12, $R \neq \{0\}$ is a field $\iff$ (0) is a maximal ideal.

2) In $\mathbb{Z}$, an ideal $(n) = \langle n \rangle$, where $n \geq 0$, is a prime ideal if and only if $n = 0$ or $n = p$ is a prime number. It is a maximal ideal if and only if $n = p$ is a

prime number. To see this last statement, note in general that, for $n \in \mathbb{Z}$ and $a \in \mathbb{Z}$, $a \in (n) \iff n$ divides a. Suppose that (p) is contained in an ideal J of $\mathbb{Z}$. Since J is in particular an additive subgroup, it is cyclic, and so $J = \langle n \rangle = (n)$ for some $n \geq 0$. Then n divides p. Then either $n = 1$, in which case $(n) = (1) = \mathbb{Z}$, or $n = p$, in which case $(n) = (p)$. It then follows that (p) is also a prime ideal; of course, it is easy to check this directly, using the basic fact that, if a prime p divides a product of two integers r, s, then it divides at least one of r, s.

Conversely, if $n \in \mathbb{N}$ is not a prime, then it is easy to see that (n) is not a prime ideal and hence is not maximal: writing $n = ab$ with $1 < a < n$, $1 < b < n$, it follows that $ab \in (n)$ but neither a nor b lies in (n). Hence (n) is not a prime ideal.

3) If F is a field and $R = F[x_1, x_2]$, then the ideals (0) and (x_1) are prime ideals in R but are not maximal, whereas (x_1, x_2) is a maximal ideal in R (it is the kernel of the surjective homomorphism $\mathrm{ev}_{0,0} \colon F[x_1, x_2] \to F$). However, it is easy to see that (x_1, x_2) is not a principal ideal, i.e. is not of the form (f) for some $f \in F[x_1, x_2]$. This says in particular that there is no polynomial f such that x_1 and x_2 are both multiples of f.