26 Homomorphisms, Ideals and Factor Rings

A historical example

You've almost certainly pondered, or been asked, the question, "What is i?" This is not easy to answer, especially once you consider some history. In the 1500's, Italian mathematicians such as Cardano posited the existence of an object, now called i, which 'solved' the equation $x^2 = -1$. Even to Cardano and his contemporaries this was an absurdity: they didn't believe that such solutions meant anything. Rather it was an early example of doing math for the sake of math: they simply applied the basic rules of algebra and computed, so that, for example,

$$(2i+1)^2 - 2(2i+1) + 5 = 0$$

Using such algebra, they found formulas for solving all quadratic, cubic and quartic polynomial equations. Over the centuries, the uses of complex numbers expanded, from early 2D analytic geometry to the multitude of modern engineering applications. However, to many mathematicians, the essential problem remained. The applications brought us no closer to understanding what i is. To modern mathematicians, it isn't good enough simply to pull i out of thin air: we want to *construct* it, and the complex numbers in a natural way, as befits their highly useful status.

The modern approach to this problem uses our rings of polynomials. Rather than solving the equation $x^2 = -1$, we define an equivalence relation on the ring of polynomials $\mathbb{R}[x]$ so that $x^2 \sim -1$. Then, almost tautologically, the equivalence class of x itself 'solves' the equation! Here is the rough idea:

- To force $x^2 \sim -1$, we define $f \sim g \iff (x^2+1) \mid (f(x) - g(x))$. Otherwise said, f and g lie in the same *coset* of the subring $\langle x^2+1 \rangle \leq \mathbb{R}[x]$ of multiples of x^2+1.
- The set of cosets $\mathbb{R}[x] \Big/ \langle x^2+1 \rangle$ naturally has the structure of a ring (indeed a field in this case).
- The evaluation homomorphism

  $$\phi_{x+\langle x^2+1\rangle} : \mathbb{R}[x] \to \mathbb{R}[x] \Big/ \langle x^2+1 \rangle : f(x) \mapsto f\big(x + \langle x^2+1 \rangle\big)$$

  maps the polynomial x^2+1 to the zero coset in the factor ring. We've therefore *constructed* a new field $\mathbb{R}[x] \Big/ \langle x^2+1 \rangle$ which contains a zero of the polynomial x^2+1.
- The complex numbers $\mathbb{C}$ can now be *defined* as this new field, and i as the coset $x + \langle x^2+1 \rangle$!

To be sure, there are many details to iron out before the above is watertight, but take a deep breath anyway for this is a triumph of mathematics. We've done what Cardano et al could not and *explicitly constructed* $\mathbb{C}$ and i in a purely algebraic manner. The next time someone asks you, "What *is* i?", you now know what to say:[1]

"i is the coset of x in the factor ring $\mathbb{R}[x] \Big/ \langle x^2+1 \rangle$!"

[1] If you want to lose friends, deliver this line with an air of smugness. If you don't yet think this is astounding, keep reading: eventually you'll learn to drink the kool-aid :)

Our primary purpose in this course is to make this discussion solid in the general context of a polynomial f over an arbitrary field $\mathbb{F}$. We start by considering...

Factor Rings

Recall the concept of a *factor group*: If N is a normal subgroup of G then the set of left cosets

$$G/N = \{xN : x \in G\}$$

forms a group under the natural operation

$$xN \cdot yN := (xy)N \qquad (*)$$

In group theory, we discovered the following:

$$\begin{aligned} N \text{ is a normal subgroup} &\iff \text{The operation } (*) \text{ is well-defined} \\ &\iff \text{There exists a homomorphism } \phi \text{ for which } \ker\phi = N \end{aligned}$$

We moreover observed the 1st isomorphism theorem $G/\ker\phi \cong \operatorname{Im}\phi$.

Our first goal is to replicate the above discussion for *factor rings* and to recognize the relationship between kernels of homomorphisms and the *ideal subrings* which play the ring-theoretic role of normal subgroups. Here is an easy example before we construct everything abstractly.

Example Consider the subring $4\mathbb{Z} \leq \mathbb{Z}$. We already know how to find the cosets of $4\mathbb{Z}$ from group theory: indeed $4\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$ and we have the factor group

$$(\mathbb{Z},+)/(4\mathbb{Z},+) = \{4\mathbb{Z}, 1+4\mathbb{Z}+1, 2+4\mathbb{Z}, 3+4\mathbb{Z}\} = \{[0],[1],[2],[3]\}$$

Since $\mathbb{Z}$ is abelian, the factor group is also abelian (indeed it is isomorphic to $(\mathbb{Z}_4,+)$). In fact we also have a natural *ring* structure: define

$$(x+4\mathbb{Z})(y+4\mathbb{Z}) := xy+4\mathbb{Z} \quad \text{alternatively} \quad [x]\cdot[y] := [xy]$$

It should be clear that this multiplication is well-defined:[2]

$$[x+4a]\cdot[y+4b] = [xy+4(ay+bx+4ab) = [xy]$$

and that $\mathbb{Z}/4\mathbb{Z}$ is therefore naturally ring-isomorphic[3] to $\mathbb{Z}_4$.

Finally note that the function $\phi : \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} : x \mapsto [x]$ is a ring-homomorphism which satisfies

$$\phi(x) = [0] \iff x \in 4\mathbb{Z}$$

Otherwise said, the subring $4\mathbb{Z}$ is the *kernel* of the homomorphism ϕ.

[2]This *requires* the important fact that $xz, zx \in 4\mathbb{Z}$ for every $x \in \mathbb{Z}$ and $z \in 4\mathbb{Z}$: the subring $4\mathbb{Z}$ is *absorptive* under multiplication. This is a stronger condition than merely being a normal subgroup and is what we shall mean by an *ideal subring*.

[3]This is really the *definition* of $\mathbb{Z}_4$ as a ring!

Homomorphisms

We quickly refresh the notion of a homomorphism of rings. Most of this is a rapid rehash of results from group theory with which you should already be comfortable.

Definition 26.1. Let R, S be rings. A function $\phi : R \to S$ is a homomorphism if

$$\forall x, y \in R, \quad \phi(x+y) = \phi(x) + \phi(y) \quad \text{and} \quad \phi(xy) = \phi(x)\phi(y)$$

The *kernel* of ϕ is the set

$$\ker \phi = \phi^{-1}(0) = \{x \in R : \phi(x) = 0\}$$

If T is a subring of R (or subset more generally), its image is

$$\phi(T) = \{\phi(x) : x \in T\}$$

The *image* or *range* of ϕ is $\operatorname{Im} \phi = \phi(R)$.
A homomorphism is an *isomorphism* if it is also bijective.

Theorem 26.2 (Basic facts)**.** *Let $\phi : R \to S$ be a ring homomorphism.*

1. *$\phi : (R, +) \to (S, +)$ is a homomorphism of groups. In particular,*

   $$\phi(0_R) = 0_S \quad \textit{and} \quad \forall x \in R,\ \phi(-x) = -\phi(x)$$

2. *$\ker \phi$ is a subring of R*
3. *ϕ is injective if and only if $\ker \phi = \{0\}$*
4. *If T is a (commutative) subring of R, then $\phi(T)$ is a (commutative) subring of S*
5. *If R has a unity 1_R, then $\phi(1_R)$ is a unity for the image $\phi(R)$*
6. *If $u \in R^\times$ is a unit then $\phi(u) \in \phi(R)^\times$ is a unit. In such a case, $\phi(u^{-1}) = [\phi(u)]^{-1}$. We can reverse the implication if ϕ is injective.*

We omit the proofs: you should write all these out as easy exercises!

Examples

1. Let $\phi : \mathbb{Z} \to \mathbb{Z}_7$ be the ring homomorphism defined by $\phi(x) = x \mod 7$. Clearly $\ker \phi = 7\mathbb{Z}$ is a subring of $\mathbb{Z}$.
2. Let $R = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$. You should check that

   $$\phi : \mathbb{C} \to R : a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

   is an *isomorphism* of fields. Being injective, its kernel is $\{0\} \leq \mathbb{C}$. The unity of R is the identity matrix, clearly equal to $\phi(1)$.

Cosets and Factor Groups

Definition 26.3. Let R be a ring and suppose that N is a subring. Let $a \in R$. The *coset* of N containing a is the set

$$a + N = \{a + h : h \in N\}$$

Note that left- and right-cosets are always equal since $(R, +)$ is abelian, whence $(N, +)$ is always a *normal subgroup* of $(R, +)$.

The following should be easy to recall from group theory: prove it yourself if you've forgotten!

Lemma 26.4. *$a + N = b + N \iff a - b \in N$. Moreover, $\sim$ defined by*

$$a \sim b \iff a - b \in N$$

is an equivalence relation on N.

As in group theory, our goal is to define a natural ring structure on the set of cosets

$$R/_N := R/_\sim = \{x + N : x \in R\}$$

where H is a subring of R. Since $(R, +)$ is abelian we know that $(N, +)$ is a normal subgroup of $(R, +)$ whence the operation of addition of cosets

$$(a + N) + (b + N) := (a + b) + N$$

is well-defined. Our attention turns to multiplication. We require the well-definition of

$$(a + N) \cdot (b + N) := ab + N$$

This is if and only if $\forall a, b \in R,\ \forall m, n \in N$,

$$\begin{aligned}(a + m)(b + n) + N = ab + H &\iff (ab + mb + an + mn) - ab \in N \\ &\iff mb + an \in N\end{aligned}$$

In particular we require:

Left-absorption: $\forall a \in R,\ n \in N$ we have $an \in N$ (let $b = m = e \in N$)

Right-absorption: $\forall b \in R,\ m \in N$ we have $mb \in N$ (let $a = n = e \in N$)

We formalize this notion.

Definition 26.5. A subring[4] $N \leq R$ is an *ideal* of R if it is left- and right-absorptive:

$$\forall x \in R,\ y \in N,\ xy \in N \text{ and } yx \in N$$

We can summarize everything in a single result.

[4]It is enough to assume that $(N, +)$ is a subgroup of $(R, +)$ with the absorptive properties: N is then automatically a subring of R, since absorption implies closure under multiplication.

Theorem 26.6. *Let N be a subring of R. The natural structure $\left(R/N, +, \cdot\right)$ is a well-defined ring if and only if N is an ideal.*

Proof. The above discussion shows that the natural operations are well-defined if and only if N is an ideal. It remains to check the ring axioms.

Since $(N,+) \triangleleft (R,+)$ it follows that $\left(R/N, +\right)$ is an abelian factor group.

Certainly $\left(R/N, \cdot\right)$ is associative due to the associativity of $(R,\cdot)$:

$$(x+N)\big((y+N)(z+N)\big) = \cdots = xyz + N = \cdots = \big((x+N)(y+N)\big)(z+N)$$

Finally, the distributivity laws carry over from R. For instance,

$$\begin{aligned}(x+N)\big((y+N)+(z+N)\big) &= (x+N)(y+z+N) = x(y+z)+N \\ &= (xy+xz)+N = (xy+N)+(xz+N) \\ &= (x+N)(y+N)+(x+N)(z+N)\end{aligned}$$

■

Examples

1. In the integers, the subring $n\mathbb{Z}$ of all multiples of n is an ideal. Indeed

   $$\forall x \in \mathbb{Z}, ny \in n\mathbb{Z} \quad \text{we have} \quad x \cdot ny = ny \cdot x = nxy \in n\mathbb{Z}$$

   It follows that $\mathbb{Z}/n\mathbb{Z}$ is a factor ring. Indeed this is the natural *definition* of the ring $\mathbb{Z}_n$.

2. In the ring $\mathbb{R}[x]$ of polynomials with real coefficients, the set

   $$\langle x^2+1\rangle := \{(x^2+1)p(x) : p(x) \in \mathbb{R}[x]\}$$

   is an ideal whence we obtain the factor ring $\mathbb{R}[x]/\langle x^2+1\rangle$ from our motivational example.

We'll revisit both these examples in more detail, and see many more examples, later.

Kernels and Ideals: the Fundamental Homomorphism Theorem

The primary result to which we are building is the ring-theoretic version of the *first isomorphism theorem.* The basic idea is that a subring is an ideal if and only if it is the kernel of some ring homomorphism.

First consider the cosets of a kernel: if $\phi : R \to S$ is a homomorphism then

$$b \in a + \ker\phi \iff b - a \in \ker\phi \iff \phi(b-a) = 0 \iff \phi(a) = \phi(b)$$

Otherwise said, the subring $\ker\phi = \phi^{-1}(0)$ has cosets

$$a + \ker\phi = \phi^{-1}[\phi(a)] = \{x \in R : \phi(x) = \phi(a)\}$$

Distinct cosets thus correspond precisely to distinct elements in the image of ϕ...

Theorem 26.7 (Fundamental Homomorphism Theorem)**.** *Every kernel of a homomorphism is an ideal and vice versa. Specifically:*

1. *Let $\phi : R \to S$ be a homomorphism of rings. Then* $\ker\phi$ *is an ideal of R and*

   $$R\Big/_{\ker\phi} \cong \operatorname{Im}\phi$$

   via the isomorphism $\mu(x + \ker\phi) := \phi(x)$.

2. *Let N be an ideal of R. Then $\gamma(x) = x + N$ defines a surjective ring-homomorphism*[5] *$\gamma : R \to R\Big/_N$ with* $\ker\gamma = N$.

Proof. We already know that all group-theoretic parts of the Theorem hold: ϕ is a group homomorphism, $\ker\phi$ is a normal subgroup of $(R, +)$, etc. We therefore check only the parts which are new for rings.

1. Let $x \in R$ and $y \in \ker\phi$. Then

   $$\phi(xy) = \phi(x)\phi(y) = 0 \implies xy \in \ker\phi$$

   Similarly $yx \in \ker\phi$, whence $\ker\phi$ is an ideal of R.
   We check that μ is a multiplicative homomorphism:

   $$\begin{aligned}\mu\Big((x+\ker\phi)(z+\ker\phi)\Big) &= \mu(xz+\ker\phi) = \phi(xz)\\ &= \phi(x)\phi(z) = \mu(x+\ker\phi)\mu(z+\ker\phi)\end{aligned}$$

2. We check that γ is a multiplicative homomorphism:

   $$\gamma(xy) = xy + N = (x+N)(y+N) = \gamma(x)\gamma(y)$$

∎

Example $\gamma : \mathbb{Z} \to \mathbb{Z}_n : x \mapsto x \mod n$ is a homomorphism with kernel $n\mathbb{Z}$. If we take the *definition* of $\mathbb{Z}_n$ to be the factor ring $\mathbb{Z}\Big/_{n\mathbb{Z}}$, then γ is precisely the canonical homomorphism in part 2. of the Fundamental Theorem.

Back to the past: 'solving' $x^2 + 1 = 0$

We now have enough machinery to properly work our motivating example.

- $N := \langle x^2 + 1\rangle$ is an ideal in the ring $\mathbb{R}[x]$.
- If $f \in \mathbb{R}[x]$ has degree ≥ 2, we may apply the division algorithm to compute

  $$f(x) = (x^2+1)q(x) + r(x) \quad \text{where} \quad \deg(r) \leq 1$$

  f and r clearly have the same coset in the factor ring $\mathbb{R}[x]\Big/_N$. We conclude that *in each coset there is a unique representative $r(x)$ of degree ≤ 1.*

[5] γ is known as the *canonical* or *fundamental homomorphism.*

- The factor ring operations are easy for these representatives:

  $$\big(a+bx+N\big)+\big(c+dx+N\big)=(a+c)+(b+d)x+N$$

  and

  $$\begin{aligned}\big(a+bx+N\big)\big(c+dx+N\big)&=ac+(ad+bc)x+bdx^2+N\\&=(ac-bd)+(ad+bc)x+N\qquad\text{(since } x^2+N=-1+N\text{)}\end{aligned}$$

  If a and b are not both 0, we quickly see that

  $$(a+bx+N)^{-1}=\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}x+N$$

  whence the factor ring is a *field*. The addition and multiplication are precisely what we expect to see for the complex numbers, so this could be taken as a *definition*: $\mathbb{C}:=\mathbb{R}[x]\Big/\big\langle x^2+1\big\rangle$

- The evaluation homomorphism $\phi_{x+\langle x^2+1\rangle}:\mathbb{R}[x]\to\mathbb{R}[x]\Big/\big\langle x^2+1\big\rangle$ returns

  $$\phi_{x+\langle x^2+1\rangle}(x^2+1)=x^2+1+\big\langle x^2+1\big\rangle=\big\langle x^2+1\big\rangle$$

  precisely the zero in the quotient ring! Otherwise said, the coset $x+\big\langle x^2+1\big\rangle$ is a zero of x^2+1 and thus plays the role of $i\in\mathbb{C}$.

For the algebraic purist, we need no more than the above: $\mathbb{C}$ *is* the factor ring, and i *is* the coset of x. This doesn't feel satisfying to most of us, particularly when we've been working with $\mathbb{C}$ and i for years. Instead, therefore, let us suppose that we were already in possession of some other nice definition of these concepts. Consider the evaluation homomorphism

$$\phi_i:\mathbb{R}[x]\to\mathbb{C}:f(x)\mapsto f(i)$$

We compute its kernel: if $f(i)=0$, then $0=\overline{f(i)}=f(\bar{i})=f(-i)$, since the coefficients of f are real numbers. But then, by the factor theorem in $\mathbb{C}[x]$, the polynomial $f(x)$ is divisible by the product $(x-i)(x+i)=x^2+1$. It follows that

$$\ker\phi_i=\big\langle x^2+1\big\rangle$$

Moreover, ϕ_i is *surjective*, since $a+ib=\phi_i(a+bx)$. The Fundamental Homomorphism Theorem then says that

$$\mathbb{R}[x]\Big/\big\langle x^2+1\big\rangle=\mathbb{R}[x]\Big/_{\ker\phi_i}\cong\operatorname{Im}\phi_i=\mathbb{C}$$

via the isomorphism

$$\mu:f(x)+\big\langle x^2+1\big\rangle\mapsto f(i)$$

More explicitly, using the unique deg ≤ 1 representative of each coset, we have

$$\mu\Big(a+bx+\big\langle x^2+1\big\rangle\Big)=a+ib$$

In essence, the Fundamental Homomorphism Theorem says that whatever alternative definition or visualization you might have of $\mathbb{C}$, it is isomorphic to ours. Whew!

27 Prime and Maximal Ideals

The previous discussion of the algebraic construction of $\mathbb{C}$ is fairly easily generalizable. For instance, given a polynomial $p(x) \in \mathbb{F}[x]$ over some field $\mathbb{F}$, we may construct the factor ring $\mathbb{F}[x]/\langle p(x) \rangle$. We'd like to know when this factor ring is a field, *without* performing an explicit calculation. In order to answer this question, and others, we consider various types of ideals that might be possessed by a given ring and consider several further examples.

Definition 27.1. Let N be an ideal of ring R.

- N is *trivial* if $N = \{0\}$.
- N is *proper* if $N \neq R$. We might write $N < R$ in this case.
- A proper ideal N is *maximal* if there is no proper ideal which properly contains N. Otherwise said, if M is an ideal such that $N \leq M < R$, then $N = M$.
- Suppose R is commutative.[6] A proper ideal N is *prime* if

$$xy \in N \implies x \in N \text{ or } y \in N$$

- Suppose R is unital and commutative. An ideal N is *principal* if there exists $x \in R$ such that $N = \{rx : r \in R\}$. We write $N = \langle x \rangle$: this is the *principal ideal generated by* x.

Principal ideals are, arguably, the simplest type of ideal: like cyclic groups, they are generated by a single element. It is easy to check that $\langle x \rangle$ is indeed an ideal:

- $0 = 0x \in \langle x \rangle$
- $\forall r, s \in R,\ rx - sx = (r - s)x \in \langle x \rangle$
- $\forall r, s \in R,\ r(sx) = (rs)x = (sx)r \in \langle x \rangle$

The third argument shows both the closure of $\langle x \rangle$ under multiplication (thus $\langle x \rangle \leq R$) *and* the absorption properties. Note how the commutativity of R justifies the right-absorption property. The notion of principal ideal becomes more difficult for non-commutative rings, so we ignore it. We require a unital ring mainly so that $x \in \langle x \rangle$!

A given ideal can satisfy several of these criteria simultaneously! We'll consider our main examples of interest (the rings $\mathbb{Z}$, $\mathbb{Z}_n$ and $\mathbb{F}[x]$) more fully shortly; first here are some other examples.

Examples

1. Every ring R has at least two ideals: R itself and the trivial ideal $\{0\}$. These lead to the rather uninteresting factor rings

$$R/R \cong \{0\} \quad \text{and} \quad R/\{0\} \cong R$$

   Certainly $\{0\} = \langle 0 \rangle$ is always a principal ideal in any ring. Moreover, if R has a unity, then $R = \langle 1 \rangle$ is also principal. If $\mathbb{F}$ is a field, then its only ideals are itself and the trivial ideal.

[6] Prime ideals can be defined for non-commutative rings, but they are more subtle and beyond our current concern.

2. The Gaussian integers $\mathbb{Z}[i] = \{x + iy : x, y \in \mathbb{Z}\}$ have many ideals. In fact it can be shown that all these are principal: for example

$$\langle 3 - i \rangle = \{(x + iy)(3 - i) = (3x + y) + (3y - x)i : x, y \in \mathbb{Z}\}$$

We can play similar games in other rings such as $\mathbb{Z}[\sqrt{2}]$.

3. Finding examples of non-principal ideals of commutative unital rings is a little tricky. Here are two standard examples:

   (a) In the ring $\mathbb{Z}[x]$ of polynomials, the subring of polynomials of the form

   $$a_0 + a_1 x + a_2 x^2 + \cdots \quad : a_0 \text{ is } \textit{even}$$

   is a non-principal ideal.

   (b) In the ring $R[x, y]$ of polynomials in two indeterminates, the subring generated by x and y is a non-principal ideal: that is simply the subring of polynomials with zero constant term.

Ideal structure in $\mathbb{Z}$

Principal ideals Every additive subgroup of $\mathbb{Z}$ is cyclic and thus has a generator n, which we may assume is non-negative. It follows that the only *subrings* of $\mathbb{Z}$ are those rings $\langle n \rangle = n\mathbb{Z}$ where $n \in \mathbb{N}_0$. We've already seen that these are all *principal ideals*, whence every ideal in $\mathbb{Z}$ is principal.

Prime ideals The ideal $p\mathbb{Z}$ is prime if and only if $p \in \mathbb{N}_0$ is prime or zero. To see this, first observe that if p is prime, then

$$xy \in p\mathbb{Z} \implies p \mid xy \implies p \mid x \text{ or } p \mid y \implies x \in p\mathbb{Z} \text{ or } y \in p\mathbb{Z}$$

where the *definition* of p being prime is in red. The primality of the trivial ideal $\{0\}$ is simpliy the statement that $\mathbb{Z}$ is an integral domain.
If $n \geq 2$ is composite ($n = ab$ where $a, b \geq 2$), then $ab \in n\mathbb{Z}$ but neither a nor b lies in $n\mathbb{Z}$. Finally $1\mathbb{Z} = \mathbb{Z}$ is not proper and so isn't prime.

Maximal ideals If $n = ab$ then $n\mathbb{Z} \in a\mathbb{Z}$. It follows that the maximal ideals in $\mathbb{Z}$ are precisely those ideals $p\mathbb{Z}$ where p is prime: thus maximal $\implies$ prime.

Factor Rings Since all ideals are principal, we've therefore found *all* the factor rings of $\mathbb{Z}$.

$$\mathbb{Z}/n\mathbb{Z} \cong \begin{cases} \mathbb{Z} & \text{if } n = 0 \\ \mathbb{Z}_n & \text{if } n > 0 \end{cases}$$

The second case includes $n = 1$ with $\mathbb{Z}_1 = \{0\}$. These can be viewed in the language of the Fundamental Homomorphism Theorem via $\phi(x) = x$ and $\phi(x) = x \mod n$ respectively. Observe that the factor ring is a field if and only if $n\mathbb{Z}$ is a maximal ideal, and an integral domain if and only if $n\mathbb{Z}$ is a prime ideal. In all cases the factor rings are commutative rings with unity.

General Ideal Structure

Many of the observations made regarding the ideal structure of $\mathbb{Z}$ are true in general. The first result should be obvious without proof.[7]

Lemma 27.2. *Let R be a ring with ideal N.*

1. *If R is commutative, then R/N is commutative.*
2. *If R has a unity 1, then $1 + N$ is a unity in R/N. Moreover units correspond:*

$$u \in R^\times \implies u + N \in \left(R/N\right)^\times$$

By considering the factor rings of $\mathbb{Z}$, we shouldn't expect any stronger structure (e.g., that of an integral domain or field) to automatically carry over to a factor ring. We can make several general conclusions.

Theorem 27.3. *Suppose R is a commutative ring with unity with ideals M and N. Then:*

1. *M is maximal $\iff$ R/M is a field.*
2. *N is prime $\iff$ R/N is an integral domain.*
3. *M maximal $\implies$ M prime.*

Proof. 1. Suppose M is a proper ideal of R with resulting factor ring R/M.

($\Rightarrow$) If the factor ring is not a field, then $\exists a \in R \setminus M$ such that $a + M$ is not a unit. Define $N = \{ra + m : r \in R, m \in M\}$. This is clearly a subring, indeed an *ideal*, of R. Since $a + M$ is not a unit we see that $ra \notin 1 + M$ for any $r \in R$, whence $1 \notin N$. It follows that N is a proper ideal of R and M is not maximal.

($\Leftarrow$) Suppose M is not maximal. Then there exists an ideal N such that $M < N < R$. Suppose that $a \in N \setminus M$ and consider the *non-zero* coset $a + M \in R/M$. If the coset were a unit, then $\exists b \in R$ such that $ab \in 1 + M$. However, N is an ideal, whence $ab \in N$. Since $M \leq N$ we conclude that $1 \in N$. But then $R = \langle 1 \rangle \leq N$: a contradiction. Thus $a + M$ is a non-zero non-unit and so R/M is not a field.

2. Suppose N is a proper ideal of R with resulting factor ring R/N. Then

$$\begin{aligned} R/N \text{ is not an integral domain} &\iff \exists a, b \in R \setminus N \text{ with } (a+N)(b+N) = ab + N = N \\ &\iff \exists a, b \notin N \text{ with } ab \in N \\ &\iff N \text{ is not prime.} \end{aligned}$$

3. M maximal $\iff$ R/M is a field $\implies$ R/M is an integral domain $\iff$ M is prime.

■

[7] It is a good exercise to see how both parts of the lemma follow from our basic properties of homomorphisms (Theorem 26.2) and the Fundamental Homomorphism Theorem.

Ideal structure in $\mathbb{Z}_n$

Principal ideals Every ideal is principal and has the form $\langle d \rangle$ where $d \mid n$. This is immediate from the fact that all *additive subgroups* of $\mathbb{Z}_n$ have this form.

Prime ideals These include the ideals $\langle p \rangle \leq \mathbb{Z}_n$ where p is a prime divisor of n. The argument is similar to that for the integers: suppose that p is a prime divisor of n, then

$$\begin{aligned} xy \in \langle p \rangle &\implies xy = pk \in \mathbb{Z}_n, \text{ for some } k \in \mathbb{Z} \\ &\implies xy = pl, \text{ for some } l \in \mathbb{Z} \text{ (since } p \mid n) \\ &\implies p \mid xy \implies p \mid x \text{ or } p \mid y \\ &\implies x \in \langle p \rangle \text{ or } y \in \langle p \rangle \end{aligned}$$

If m is a composite divisor of n, then $\exists a, b \notin \langle m \rangle$ such that $ab = m \in \langle m \rangle$.
Additionally, it is possible that the trivial ideal $\langle 0 \rangle$ is prime, but *only* if $\mathbb{Z}_n$ is an integral domain: i.e. if n is itself prime!

Maximal ideals These are identical to the prime ideals: if $a \mid b$ and $b \mid n$ where b is a proper divisor of n, then $\langle b \rangle \leq \langle a \rangle$. If n is prime, then the only prime/maximal ideal is the trivial ideal $\{0\}$.

Factor rings Putting this together, we see that, for any divisor $d \mid n$,

$$\mathbb{Z}_n \Big/ \langle d \rangle = \{ \langle d \rangle, 1 + \langle d \rangle, \ldots, d - 1 + \langle d \rangle \} \cong \mathbb{Z}_d$$

The fact that $\mathbb{Z}_d$ is a field if and only if d is prime fits with the description of the maximal ideals. Moreover, if $n = p$ is prime, then taking $d = 0$ trivially yields the field $\mathbb{Z}_p$.

Here are two concrete examples: first we take the ideals and factor rings of $\mathbb{Z}_{12}$:

- $N = \langle 1 \rangle = \mathbb{Z}_{12}$, and $\mathbb{Z}_{12} \Big/ N = \{\mathbb{Z}_{12}\} \cong \mathbb{Z}_1$ is trivial.
- $N = \langle 2 \rangle$ is prime/maximal, $\mathbb{Z}_{12} \Big/ \langle 2 \rangle = \{ \langle 2 \rangle, 1 + \langle 2 \rangle \} \cong \mathbb{Z}_2$ is a field.
- $N = \langle 3 \rangle$ is prime/maximal, $\mathbb{Z}_{12} \Big/ \langle 3 \rangle = \{ \langle 3 \rangle, 1 + \langle 3 \rangle, 2 + \langle 3 \rangle \}$ is a field.
- $N = \langle 4 \rangle$ has $\mathbb{Z}_{12} \Big/ \langle 4 \rangle \cong \mathbb{Z}_4$ is not a field.
- $N = \langle 6 \rangle$ has $\mathbb{Z}_{12} \Big/ \langle 6 \rangle \cong \mathbb{Z}_6$ is not a field.
- $N = \langle 0 \rangle$ has $\mathbb{Z}_{12} \Big/ \langle 0 \rangle \cong \mathbb{Z}_{12}$ is not a field.

Now consider the ideals/factor rings in $\mathbb{Z}_{17}$. We have merely

$$\mathbb{Z}_{17} \Big/ \langle 1 \rangle = \mathbb{Z}_{17} \Big/ \mathbb{Z}_{17} \cong \mathbb{Z}_1 \quad \text{and} \quad \mathbb{Z}_{17} \Big/ \{0\} \cong \mathbb{Z}_{17}$$

In both cases this fits with the theorem.

Ideals in $\mathbb{F}[x]$

Our primary interest is in factor rings of $\mathbb{F}[x]$ where $\mathbb{F}$ is a field. First note something which should be obvious: if $f, g \in \mathbb{F}[x]$, then

$$f \mid g \iff \exists q \in \mathbb{F}[x] \text{ such that } g = qf \iff g \in \langle f(x) \rangle \qquad (*)$$

Theorem 27.4. *Let $\mathbb{F}$ be a field.*

1. *Every ideal of $\mathbb{F}[x]$ is principal.*
2. *The principal ideal $\langle f(x) \rangle$ is maximal if and only if f is irreducible. Otherwise said, $\mathbb{F}[x]/\langle f(x) \rangle$ is a field if and only if f is irreducible.*
3. *The principal ideal $\langle f(x) \rangle$ is prime if and only if f is prime.*

Proof. 1. Suppose $N \leq \mathbb{F}[x]$ is a non-trivial ideal (the trivial ideal is certainly principal!). Let $g(x)$ be any non-zero polynomial of minimal degree in N and let $f(x) \in N$. Apply the division algorithm:

$$f(x) = q(x)g(x) + r(x), \quad \deg r < \deg g$$

Clearly $r(x) = f(x) - q(x)g(x) \in N$: by minimality, $r(x)$ must be the zero polynomial. We conclude that $N = \langle g(x) \rangle$ is principal.

2. If $f(x) = g(x)h(x)$ is reducible over $\mathbb{F}$, then $f \in \langle g(x) \rangle \implies \langle f(x) \rangle \leq \langle g(x) \rangle$ whence $\langle f(x) \rangle$ is not maximal.
Conversely, suppose $\langle f(x) \rangle$ is non maximal. Then, since every ideal is principal, there exists a proper ideal $\langle g(x) \rangle < \mathbb{F}[x]$ properly containing $\langle f(x) \rangle$. Clearly $g \mid f$. Moreover,
   - g is a proper divisor of f, else f, g are associates and the ideals are equal!
   - g is not a unit, else $\langle g(x) \rangle = \mathbb{F}[x]$ is non-proper.

   We conclude that f is reducible.

3. Compare the definitions:

   f prime: $\quad f \mid gh \implies f \mid g$ or $f \mid h$
   $\langle f(x) \rangle$ prime: $\quad gh \in \langle f(x) \rangle \implies g \in \langle f(x) \rangle$ or $h \in \langle f(x) \rangle$

   The left and right sides of these implications are equivalent by $(*)$.

■

Corollary 27.5. *Theorems 27.3 and 27.4 combine to show that, in $\mathbb{F}[x]$, if f is irreducible then it is prime. Since every prime is irreducible in an integral domain (of which $\mathbb{F}[x]$ is one), we see that the notions are equivalent.*

The Corollary allows us to prove the uniqueness part of the unique factorization theorem in $\mathbb{F}[x]$ *without* invoking the Euclidean algorithm or gcd's of polynomials.

Kronecker's Theorem: victory!

We now have all the ingredients to complete our main purpose: this was first published by Leopold Kronecker in 1881, though not in this language.

Theorem 27.6 (Kronecker)**.** *Suppose $\mathbb{F}$ is a field and $f \in \mathbb{F}[x]$ is non-constant. Then there exists a field $\mathbb{E}$ containing an isomorphic copy of $\mathbb{F}$ and an element $\alpha \in \mathbb{E}$ such that $f(\alpha) = 0$.*

Proof. Suppose f is irreducible. We may then define

$$\mathbb{E} := {}^{\mathbb{F}[x]}\Big/_{\langle f(x)\rangle} \quad \text{and} \quad \alpha := x + \langle f(x)\rangle$$

Theorem 27.4 guarantees that $\mathbb{E}$ is a field, which moreover contains an isomorphic copy of

$$\mathbb{F} \cong \{a + \langle f(x)\rangle : a \in \mathbb{F}\}$$

We also see that[8]

$$f(\alpha) = \phi_\alpha(f(x)) = f(x) + \langle f(x)\rangle = \langle f(x)\rangle = 0_{\mathbb{E}}$$

If f is reducible, we may repeat the above for any irreducible factor g of f. Clearly any zero of g is also a zero of f. ∎

As a sanity check, you should convince yourself that if $\deg(f) = 1$, then the field $\mathbb{E}$ in the proof is isomorphic to $\mathbb{F}$ itself!

Aside: Prime Fields; characteristics revisited

Theorem 27.7. *Suppose R is a unital ring with $\operatorname{char}(R) = n$. Then the set*

$$S := \{x \cdot 1 : x \in \mathbb{Z}\}$$

forms a subring of R isomorphic to $\mathbb{Z}_n$, or to $\mathbb{Z}$ if $\operatorname{char}(R) = 0$.

Proof. Define $\phi : \mathbb{Z} \to R$ by $\phi(x) = x \cdot 1$. This is easily seen to be a ring-homomorphism. But then $S = \phi(\mathbb{Z})$ is a subring of R. If $\operatorname{char}(R) = 0$, then $\ker\phi = \{0\}$ whence ϕ is injective and $S \cong \mathbb{Z}$. If $\operatorname{char}(R) = n$ is positive, then $\ker\phi = n\mathbb{Z}$, whence

$$S = \phi(\mathbb{Z}) \cong {}^{\mathbb{Z}}\Big/_{n\mathbb{Z}} \cong \mathbb{Z}_n$$

∎

Corollary 27.8. *Recall that the characteristic of every field is either zero or a prime. If $\operatorname{char}(\mathbb{F}) = p$, then $\mathbb{F}$ contains a subfield isomorphic to $\mathbb{Z}_p$. If $\operatorname{char}(\mathbb{F}) = 0$ then $\mathbb{F}$ contains a subfield isomorphic to $\mathbb{Q}$.*

Proof. By the Theorem, we certainly have a subring isomorphic to $\mathbb{Z}_p$ or $\mathbb{Z}$. But then $\mathbb{F}$ also contains a subfield isomorphic to the field of fractions of said integral domain: namely $\mathbb{Z}_p$ or $\mathbb{Q}$. ∎

Definition 27.9. The fields $\mathbb{Z}_p$ and $\mathbb{Q}$ are called *prime fields*: they form the building-blocks of all fields in the sense that every field is a vector space over one of these. We shall explore this idea more later.

[8] If this is too quick, let $f(x) = a_n x^n + \cdots + a_0$ so that

$$f(\alpha) = a_n\alpha^n + \cdots + a_0 = a_n(x + \langle f(x)\rangle)^n + \cdots + a_0 = a_n x^n + \cdots + a_0 + \langle f(x)\rangle = \langle f(x)\rangle$$

Aside: an alternative proof of Theorem 27.3, part 1.
A more sophisticated proof of the relationship between maximal ideals and fields can be given, though it needs a few prerequisites. The crucial observation is that the canonical homomorphism allows us to transfer the relationship between ideals from R to a quotient ring. You should compare this proof with the original.

Let M be an ideal of R and consider the canonical homomorphism $\gamma : R \to {}^{R}\!/_{M} : r \mapsto r + M$. This is surjective. Observe:

- If N is an ideal of R, then the $\gamma(N)$ is an ideal of $\gamma(R) = {}^{R}\!/_{M}$ (by surjectivity).
- If $\widetilde{N}$ is an ideal of ${}^{R}\!/_{M}$, then $\gamma^{-1}(\widetilde{N}) = \{r \in R : \gamma(r) \in \widetilde{N}\}$ is an ideal of R.
- Writing $\widetilde{N} = \gamma(N)$, we have a correspondence of ideals:

  $$M \leq N \leq R \iff \{M\} \leq \widetilde{N} \leq {}^{R}\!/_{M}$$

  Indeed $M = N \iff \widetilde{N} = \{M\}$ and $N = R \iff \widetilde{N} = {}^{R}\!/_{M}$.
- Now for the proof: if ${}^{R}\!/_{M}$ is not a field, let $a + M$ be any non-zero non-unit and define the principal ideal $\widetilde{N} = \langle a + M \rangle$. This is clearly proper (it doesn't contain $1 + M$) and non-trivial ($a \notin M$), whence N is a proper ideal of R properly containing M, which is not maximal.

  Conversely, if M is not maximal, then $\exists N$ properly between M and R: construct $\widetilde{N}$, a proper, non-trivial ideal of ${}^{R}\!/_{M}$. But then ${}^{R}\!/_{M}$ is not a field, since the only ideals in a field are trivial or non-proper.