Constructions of fields

For the past few weeks we have studied general properties of rings, and described how ring theory interacts with other areas of mathematics such as geometry and number theory. For the rest of the course, we will focus our attention on field theory.

Today we will discuss a number of constructions for fields that will be useful later.

Field of fractions

Let R be any integral domain. It may not be the case that R is a field. However, we can formally "invert" all non-zero elements of R to obtain a field. The result of this construction is $\mathrm{Frac}(R)$, called the *field of fractions of* R, also called the *quotient field*.

To construct this field, we begin with the set of pairs $\{(a,b): a \in R, b \in R, b \neq 0\}$. We define an equivalence relation $\sim$ on this set as follows:

$$(a,b) \sim (c,d) \qquad \Longleftrightarrow \qquad ac - bd = 0$$

Let $\mathrm{Frac}(R)$ be the equivalence classes of this relation. It is customary to write the equivalence class of (a,b) as a/b. Then define addition and multiplication as:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad\qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

You can then check that with these operations the set $\mathrm{Frac}(R)$ satisfies the axioms of a commutative ring. Furthermore, if $a/b \in \mathrm{Frac}(R)$ is non-zero, then it has multiplicative inverse b/a. Thus $\mathrm{Frac}(R)$ is a field. The following is an exercise:

▶ **The map $\phi : R \to \mathbf{Frac}(R)$ given by $\phi(a) = a/1$ is a 1-1 ring homomorphism.**

For example, the field of fractions of the integers $\mathbb{Z}$ is naturally isomorphic to the field of rational numbers $\mathbb{Q}$, and we write $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.

If R is a field, then $\mathrm{Frac}(R)$ is naturally isomorphic to R.

For another example, consider the ring of polynomials $R[x]$ where R is an integral domain such as $\mathbb{Z}$ or $\mathbb{Q}$. Then $R[x]$ is an integral domain, and we have

$$\mathrm{Frac}(R[x]) = \left\{ \frac{f(x)}{g(x)} : \ f(x), g(x) \in R[x], \, g(x) \neq 0 \right\}$$

It is instructive to verify that this field is isomorphic to $\mathrm{Frac}(\mathrm{Frac}(R)[x])$. In other words, we can first take the field of fractions of R, then the field of fractions of $\mathrm{Frac}(R)[x]$, and we get the same result. For example, $\mathrm{Frac}(\mathbb{Z}[x])$ is isomorphic to $\mathrm{Frac}(\mathbb{Q}[x])$.

The field of fractions of R is an abstract field constructed in a way such that there is a natural "inclusion" homomorphism $R \to \mathrm{Frac}(R)$. It gives us a way of viewing any integral domain as sitting inside some larger field. In practice, we may already have R sitting inside a field, and the field of fractions is then isomorphic to something very concrete.

▶ **Suppose a ring R is contained in a field E, and F is the smallest subfield of E containing R. Then F is isomorphic to $\mathrm{Frac}(R)$.**

Proof. By assumption, $R \subset F$. We define $\phi : \mathrm{Frac}(R) \to F$ as follows: $\phi(a/b) = ab^{-1}$. This makes sense because $a \in R$ and $b \in R$; in particular, $b \in F$, so b has a multiplicative inverse. Then ϕ is a homomorphism of fields. This is a 1-1 homomorphism, as is every homomorphism between fields. Consider the image of ϕ. This is a subfield of F containing R, and so by assumption it must be equal to F. Thus ϕ is an isomorphism. □

Let $R = \mathbb{Z}[i]$, the Gaussian integers. Consider the following subfield of $\mathbb{C}$:

$$\mathbb{Q}(i) = \{a + bi : \ a, b \in \mathbb{Q}\}$$

It is not difficult to see that this is the smallest subfield of $\mathbb{C}$ which contains $\mathbb{Z}[i]$. Thus $\mathrm{Frac}(\mathbb{Z}[i])$ is isomorphic to $\mathbb{Q}(i)$.

Extension fields

Let F be a field, and E is a field containing F, i.e. $F \subset E$. In this situation E is called an *extension field* of F. The extension is *proper* if $E \neq F$.

If $\alpha \in E$ we write $F(\alpha) \subset E$ for the smallest field inside E containing both F and α.

For example, let $F = \mathbb{Q}$, $E = \mathbb{C}$, $\alpha = i = \sqrt{-1}$. Then $\mathbb{Q}(i)$ is the smallest field contained in $\mathbb{C}$ which contains both $\mathbb{Q}$ and i.

For a more interesting example let us consider the field

$$E = \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

This is the smallest field containing both $\mathbb{Q}$ and $\alpha = \sqrt{2} + \sqrt{3}$. Note that

$$(\sqrt{2} + \sqrt{3}) \cdot (\sqrt{2} - \sqrt{3}) = 2 - 3 = -1$$

and so the multiplicative inverse of $\sqrt{2} + \sqrt{3}$ is given by $-\sqrt{2} + \sqrt{3}$. Then

$$\frac{1}{2}\left(\alpha + \alpha^{-1}\right) = \frac{1}{2}\Big((\sqrt{2} + \sqrt{3}) + (-\sqrt{2} + \sqrt{3})\Big) = \sqrt{3}$$

so that $\sqrt{3} \in E$. Similarly, $\sqrt{2} \in E$. In particular, E is an extension field of the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$. Note $\sqrt{2} + \sqrt{3}$ is not in either of these fields, so the extension is proper.

Quotient fields

A very useful construction that can give us fields is the quotient ring R/I of some ideal I in a commutative ring R. Recall that R/I is a field if and only if I is a *maximal* ideal.

A common scenario is when the ring R is a polynomial ring of the form $F[x]$ where F itself is a field. Recall we proved that $F[x]$ is a PID in this case. We need the following:

▸ **An ideal (a) in a PID is maximal if and only if a is irreducible.**

Proof. Suppose (a) is maximal, and a is not irreducible. Then $a = bc$ where b, c are not units. Then $(a) = (bc) = (b)(c)$ where (b), (c) are proper ideals. In particular, $(a) \subset (b)$. By maximality, $(a) = (b)$. Then $a = bu$ for a unit u. We obtain $a = bu = bc$ implying $b(u - c) = 0$. Since the ring is an integral domain and $b \neq 0$, $u = c$, Contradicting that c is not a unit. Thus a is irreducible. Conversely, suppose a is irreducible, and (a) is not maximal. Then (a) is properly contained in (b) for some proper ideal (b). Then $a = bc$ for some c. As a is irreducible, one of b or c is a unit. If b is a unit, (b) is not proper. If c is a unit, then $(a) = (b)$, a contradiction. Thus (a) is a maximal ideal. □

Returning to the case of $F[x]$, where F is a field, note that the group of units of $F[x]$ is exactly the non-zero elements of F. Thus $f(x)$ is irreducible if $f(x)$ is non-zero and not a constant polynomial, and if $f(x) = g(x)h(x)$ implies that one of $g(x)$ or $h(x)$ is a constant polynomial. Recalling that $F[x]/(f(x))$ is a field when $(f(x))$ is maximal, we obtain:

▸ **For F a field and $f(x) \in F[x]$ an irreducible polynomial, $F[x]/(f(x))$ is a field.**

Let us now use this to construct some fields.

Take $F = \mathbb{R}$ and let $f(x) \in \mathbb{R}[x]$ be the irreducible polynomial $f(x) = x^2 + 1$. Then

$$\mathbb{R}[x]/(x^2 + 1)$$

is a field. We consider some elements in this field, where $I = (x^2 + 1)$:

$$\begin{aligned} x^2 + I &= -1 + I \\ x^3 + I &= -x + I \\ x^4 + I &= 1 + I \\ &\vdots \end{aligned}$$

Using these computations we see that any element $g(x) + I$ can be written as $a + bx + I$ where $a, b \in \mathbb{R}$. Noting that x behaves just like $i = \sqrt{-1} \in \mathbb{C}$, we define

$$\phi : \mathbb{C} \longrightarrow \mathbb{R}[x]/(x^2 + 1)$$

by $\phi(a + bi) = a + bx + I$, and you may verify this is an isomorphism.

For another example, let us take $F = \mathbb{Z}_2$ and let $f(x) \in \mathbb{Z}_2[x]$ be $f(x) = x^2 + x + 1$. Suppose this is reducible. Then $f(x) = (a + bx)(c + dx) = ac + (bc + ad)x + bdx^2$ for $a, b, c, d \in \mathbb{Z}_2$. But it is easily seen that no such a, b, c, d can work. Thus $f(x)$ is irreducible in $\mathbb{Z}_2[x]$.

Now we have a field given by the quotient

$$\mathbb{Z}_2[x]/(x^2 + x + 1)$$

Let us write down some elements of this field, where $I = (x^2 + x + 1)$:

$$\begin{gathered} x^2 + I = x + 1 + I \\ x^3 + I = 1 + I \end{gathered}$$

In fact we see that every element in this field is equivalent to one of the cosets corresponding to $0, 1, x, 1 + x$. Thus we have a field with 4 elements.