9 Building New Rings

9.1 Review

Last time, we introduced the idea of rings (where we can both add and multiply) and their ideals. As an aside, the term *ring* first appeared at the end of the 19th century in works by Hilbert; it's unclear why exactly he chose this term, but in the original German, the word essentially means a group of things coming together. Meanwhile, the term *ideal* comes from "ideal divisors" (we'll see later what this means).

As we saw earlier, ideals in rings work similarly to normal subgroups in groups. For an ideal $I \subset R$, we can construct the *quotient ring* R/I, and analogous versions of the theorems from group theory apply here as well. However, note that unlike the case of normal subgroups in groups, an ideal is generally not a subring. This is because it doesn't usually have 1_R — for example, $2\mathbb{Z} \subset \mathbb{Z}$ clearly doesn't contain 1. In fact, if the ideal *did* contain 1_R, it would have to be the entire ring. However, an ideal *does* satisfy the other axioms.

9.2 Product Rings

Now that we have an understanding of what rings are, we can think about how to construct them.

Guiding Question
How can we build new rings out of rings that we already have?

One construction is taking the *product* of two rings:

Definition 9.1
Let R and S be two rings. The **product ring**, denoted $R \times S$, is the set of pairs (r, s) with $r \in R$ and $s \in S$ (the Cartesian product of the two sets), along with componentwise addition and multiplication.

It's clear that the ring axioms clearly hold, with $1_{R\times S} = (1_R, 1_S)$.

Given a product ring $R \times S$, we have the **projection homomorphism** $R \times S \to R$ given by $(r, s) \mapsto r$. The kernel of this homomorphism is the set $(0, s)$ for $s \in S$. In other words, we could describe this kernel as the ideal of $R \times S$ generated by $(0, 1_S)$, since $(0, s) = (0, s) \cdot (0, 1_S)$.

Guiding Question
Given a ring Q, how can we recognize whether Q is isomorphic to $R \times S$ for some nonzero R and S?

(We ask this question about *nonzero* R and S because every ring Q is trivially the product of itself and the zero ring.)

First, if $Q = R \times S$, then we can consider the two elements $e_1 = (1_R, 0)$ and $e_2 = (0, 1_S)$. These are not units, but they are somewhat similar to units — in particular, they are *idempotent*.

Definition 9.2
An element e is **idempotent** if $e^2 = e$, or equivalently if $e(1 - e) = 0$.

Note that if e is idempotent, so is $1 - e$.

In our situation, if we have a product of two rings, then we have two idempotent elements e_1 and e_2 (which are neither 0 nor 1). We'll soon see that the converse is true as well. The intuition here may be more familiar in a linear algebra setting — suppose we have a vector space V and an idempotent matrix E, meaning that $E^2 = E$. Then its only eigenvalues are 0 and 1. So if we let V_1 and V_0 be the corresponding eigenspaces, then we can split $V = V_1 \oplus V_0$. So an idempotent matrix can be used to split the vector space into two smaller ones; it turns out it's possible to do something similar for rings.

Note that in any ring, 0 and 1 are both idempotent. In a *field*, there are no other idempotents — if $e(1 - e) = 0$, then e or $1 - e$ must be 0 — but this is not true in general, as we've just seen that there are other idempotents in $R \times S$.

Proposition 9.3
A ring Q is isomorphic to a product of rings $R \times S$ if and only if Q contains an idempotent other than 0 and 1.

Proof. We've already seen that $R \times S$ contains the idempotent elements $(1_R, 0_S)$ and $(0_R, 1_S)$, so it suffices to prove the other direction.

Given an idempotent $e \in Q$, take $R = eQ$ and $S = (1-e)Q$. Note that R (and similarly S) is a ring — it's clearly an abelian group under addition, and we can multiply the same way as in Q since

$$eq_1 \cdot eq_2 = e^2 q_1 q_2 = eq_1 q_2.$$

In particular, $e = 1_R$ (it's not a unit in the entire ring Q, but it *is* a unit in the smaller ring R). Similarly, $1 - e = 1_S$.

Then to check that $Q \cong R \times S$, for any $x \in Q$, we can write

$$x = ex + (1-e)x.$$

So then there is an isomorphism $Q \to R \times S$, given by $x \mapsto (ex, (1-e)x)$; its inverse map is given by $(r, s) \mapsto r + s$. (It's possible to explicitly check that these maps are inverses; the point is that $e(1-e) = 0$, so "mixed" terms disappear when we multiply.) □

Note 9.4
Note that R is a ring and is a subset of Q, but R is *not* a subring of Q in our terminology, since it doesn't contain 1_Q.

Similarly, the map $R \to R \times S$ sending $r \mapsto (r, 0)$ is compatible with addition and multiplication; but it is not a homomorphism in our terminology, since it does not send 1_R to $1_{R \times S}$.

Student Question. *In our construction, we took $R = eQ$ and $S = (1-e)Q$ for an idempotent e. But if Q was a field, wouldn't this require e to be 0 or 1?*

Answer. *Yes — this shows that a field cannot be written as a product of two rings (in a nontrivial way).*

Furthermore, it is possible to define the product of any collection of rings, finite or infinite, in the same way (with the operations performed componentwise).

9.3 Adjoining Elements to a Ring

A different way of creating new rings, which is quite important, is to *adjoin* elements.

Definition 9.5
If R is a subring of S, and $\alpha \in S$, then the ring $R[\alpha]$ is defined as the smallest subring of S containing both R and α.

If a subring contains R and α, then it must contain all powers of α, and therefore all linear combinations $\sum r_i \alpha^i$. Meanwhile, the set of such linear combinations is a valid subring (multiplying two such linear combinations gives us another), so $R[\alpha]$ can be explicitly described as

$$R[\alpha] = \left\{ \sum_{i=0}^{n} r_i \alpha^i \mid r_i \in R \right\}.$$

Example 9.6
When $S = \mathbb{C}$, $R = \mathbb{Z}$, and $\alpha = i$, we get the **Gaussian integers** $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

Example 9.7
We have $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. (Note that $\sqrt{2}^2 = 2$ is already in $\mathbb{Q}$, so we can ignore terms with power at least 2; the same was true in the previous example $\mathbb{Z}[i]$.)

Example 9.8
The ring $\mathbb{Z}[1/2]$ is the set of fractions whose denominator is a power of 2.

Similarly, if we start with elements $\alpha_1, \ldots, \alpha_n$ in S, then $R[\alpha_1, \ldots, \alpha_n]$ is the smallest subring of S containing R and all the α_i. It consists of all sums of products of powers of the α_i, with coefficients in R.

Student Question. *Do the powers of α (when we write elements of $R[\alpha]$) have to be finite?*

Answer. *Yes — when we write*

$$R[\alpha] = \left\{ \sum_{i=0}^{n} r_i \alpha^i \mid r_i \in R \right\},$$

there are infinitely many n to consider, but each sum itself is finite. We don't really have a way to make sense of an infinite sum here — in a ring, we can iterate the operation of addition to get finite sums, but we can't get infinite sums.

Student Question. *Are we allowed to adjoin π to $\mathbb{Z}$, and does this give $\mathbb{R}$?*

Answer. *$\mathbb{Z}[\pi]$ is definitely a legitimate example, and it's a* subring *of $\mathbb{R}$, but it's not $\mathbb{R}$ itself. The fastest way to see it's not $\mathbb{R}$ is that $\mathbb{Z}[\pi]$ is countable and $\mathbb{R}$ is not.*

9.4 Polynomial Rings

There is another way to think of adjoining elements:

Definition 9.9
Let R be a ring, and x a formal variable. Then the **polynomial ring** $R[x]$ is the set

$$R[x] = \left\{ \sum_{i=0}^{n} r_i x^i \mid r_i \in R \right\}$$

(with addition and multiplication defined in the usual way).

Note that for rings such as $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Q}$, we could instead think of $R[x]$ as the ring of polynomial *functions* from R to itself — but this doesn't work in general.

In general, given any $\alpha \in R$ and $P \in R[x]$, we can always plug in α in place of x and compute the expression $P(\alpha)$; so every polynomial does give a function from R to itself. In fact, this map is compatible with the ring structure:

Definition 9.10
For any fixed $\alpha \in R$, there is a homomorphism $R[x] \to R$ which sends $x \mapsto \alpha$; this is called the **evaluation homomorphism** at α.

Note that here we are fixing α and varying the polynomial (rather than the other way around).

So each $P \in R[x]$ yields a function $R \to R$. But in general, it carries more information than just this function — in general, it's not possible to recover the polynomial from the function. So it's better to think of polynomials in terms of the formal variable rather than in terms of functions.

Example 9.11
Consider the polynomial ring $\mathbb{F}_p[x]$, where $\mathbb{F}_p$ denotes the field $\mathbb{Z}/p\mathbb{Z}$. Even without writing down an explicit example, it is possible to see that $\mathbb{F}_p$ is a finite set, and so the space of functions from $\mathbb{F}_p$ to itself is finite-dimensional as a $\mathbb{F}_p$-vector space. But the space $\mathbb{F}_p[x]$ is infinite-dimensional, since it is spanned by powers of x. Thus, it *cannot* be possible to recover the polynomial $P \in \mathbb{F}_p[x]$ from its corresponding function.

As an explicit example, take $P(x) = x^p - x$, known as the *Artin–Schreier* polynomial. Then $\alpha^p - \alpha = 0$ for all $\alpha \in \mathbb{F}_p$ (by Fermat's Little Theorem), so the polynomial $x^p - x$ corresponds to the zero function $\mathbb{F}_p \to \mathbb{F}_p$, but is not the zero polynomial.

We can define the ring of polynomials in multiple variables — denoted $R[x_1, \dots, x_n]$ — in the same way, as formal expressions of the form

$$\sum r_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n}.$$

We can build on the idea of the evaluation homomorphism, to get an important property of polynomial rings:

Proposition 9.12 (Mapping Property)
Suppose we have a ring R, and a ring homomorphism $\varphi : R \to S$. Then given $\alpha_1, \dots, \alpha_n \in S$, there exists a unique extension of φ to a homomorphism $\widetilde{\varphi} : R[x_1, \dots, x_n] \to S$ such that $\widetilde{\varphi}(r) = \varphi(r)$ for $r \in R$, and $\widetilde{\varphi}(x_i) = \alpha_i$ for all i.

This is much less complicated than it appears. The unique extension is just evaluation — we must have

$$\widetilde{\varphi}\left(\sum r_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n}\right) = \sum \varphi(r_{i_1 \dots i_n}) \alpha_1^{i_1} \cdots \alpha_n^{i_n}$$

for any polynomial (this follows directly from the properties of a homomorphism), and this is a valid homomorphism. In some sense, all this proposition is saying is that given a polynomial and some values, we can evaluate the polynomial at those values, and this is compatible with the ring structures.

But it's important because it gives us another way of looking at our original definition of adjoining elements — if $R \subset S$ is a subring, then

$$R[\alpha_1, \dots, \alpha_n] = R[x_1, \dots, x_n] / \ker \widetilde{\varphi},$$

where φ is the inclusion map $R \hookrightarrow S$ given by $r \mapsto r$. So we can obtain our initial construction of adjoining specific elements $\alpha_i \in S$ by instead adjoining formal variables to produce a polynomial ring, and then modding out by an ideal.

Example 9.13
We have $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[x]/(x^2 - 2)$.

Example 9.14
We have $\mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$. This is a particularly good example of how we want to use this construction — in some sense, this is the *definition* of how $\mathbb{C}$ is constructed. In $\mathbb{R}$, there is no element satisfying $x^2 + 1 = 0$, so we simply define some formal variable i which *does* satisfy this equation, and in doing so, we define how $\mathbb{C}$ behaves.

This gives us an idea — we can construct new rings as the quotient of $R[x_1, \dots, x_n]$ by ideals. Sometimes in algebra, if you want an element with a certain property, you can just add in a variable and state that it satisfies the property, as in the case of defining i to be an element satisfying $i^2 = -1$ (although there is work to do in order to make this construction make sense).

This motivates us to study ideals in polynomial rings. We'll discuss this in more detail next time. But as an example, we can consider $F[x]$ for a field F (note that this is quite restrictive, as we must start with a field, and we only adjoin *one* variable). We'll see that every ideal in $F[x]$ must be principal, meaning every ideal I can be written as (P) — this will essentially follow from polynomial division with remainder. We'll then see that the construction $F[x]/(P)$ can be thought of as adjoining a root of P to F.

Resource: Algebra II Student Notes

Spring 2022

Instructor: Roman Bezrukavnikov
Notes taken by Sanjana Das and Jakin Ng