Math 332 Winter 2023, Lecture 27: Polynomials

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wa`

3. Monoid algebras and polynomials

Recall: For this entire chapter, we fix a **commutative** ring R.

3.4. Intermezzo: Quotients of R-algebras

A ring can be quotiented modulo an ideal.[1]

An R-module can be quotiented modulo a submodule.[2]

Thus, you would expect that an R-algebra (which, by its very definition, is always a ring and an R-module at the same) can be quotiented modulo an appropriate "ideal-submodule" (i.e., an ideal that happens to be an R-submodule as well).

This is indeed the case, and it's even simpler than that, because we don't even need to define these "ideal-submodules"; instead, any ideal will do, since any ideal of an R-algebra is automatically an R-submodule. Let us state this all as a theorem:

Theorem 3.4.1. Let A be an R-algebra. Let I be an ideal of A. Then:

(a) The ideal I is also an R-submodule of A.

(b) The quotient ring A/I and the quotient R-module A/I fit together to form an R-algebra.

(c) The canonical projection $\pi : A \to A/I$ (which sends each $a \in A$ to its residue class $\overline{a} = a + I$) is an R-algebra morphism (from the original R-algebra A to the R-algebra A/I that we just constructed in part **(b)**).

Proof. **(a)** We need to prove that I is closed under scaling. But this follows from the fact that

$$r \underbrace{i}_{=1_A \cdot i} = r\left(1_A \cdot i\right) = \left(r \cdot 1_A\right) i \qquad \text{for all } r \in R \text{ and } i \in I$$

(and from the fact that I is an ideal of A, so that $\left(r \cdot 1_A\right) i \in I$).

(b), **(c)** follow using standard techniques. □

Quotient R-algebras also have a universal property:

[1] That is: If S is a ring and I is an ideal of S, then there is a quotient ring S/I.

[2] That is: If M is an R-module and I is an R-submodule of M, then there is a quotient R-module M/I.

Theorem 3.4.2 (Universal property of quotient algebras, elementwise form)**.** Let A be an R-algebra. Let I be an ideal of A.

Let B be an R-algebra. Let $f : A \to B$ be an R-algebra morphism. Assume that $f(I) = 0$ (by this we mean that $f(i) = 0$ for all $i \in I$). Then, the map

$$\begin{aligned} f' : A/I &\to B, \\ \overline{a} &\mapsto f(a) \qquad \text{(for all } a \in A\text{)} \end{aligned}$$

is well-defined (i.e., the value $f(a)$ depends only on the residue class $\overline{a}$, not on a itself) and is an R-algebra morphism.

Proof. This is analogous to our proof of the universal property of quotient rings (Theorem 1.9.6 in Lecture 10). This time, we just need to discuss the scaling along with the addition and the multiplication (but it is just as easy to handle). □

3.5. Adjoining roots

3.5.1. A notation for quotients by principal ideals

We introduce a convenient shorthand notation for quotient rings modulo principal ideals:

Convention 3.5.1. Let S be any commutative ring, and let $a \in S$. Then, S/a shall mean the quotient ring S/aS.

This generalizes our shorthand notation $\mathbb{Z}/n$ for the quotient ring $\mathbb{Z}/n\mathbb{Z}$ (when n is an integer). This shorthand becomes particularly useful when S is not $\mathbb{Z}$ but something more complicated like a polynomial ring, so that you really don't want to write S twice.

We recall briefly the intuition behind quotient rings: If I is an ideal of a ring R, then R/I is "what becomes of R if we equate all elements of I to zero". Thus, in particular, the ring S/a in Convention 3.5.1 is "what becomes of S if we equate all multiples of a to zero", or, even more simply, "what becomes of S if we equate a to zero" (since equating a to zero automatically forces all multiples of a to become 0 as well). For example, $\mathbb{Z}/7$ is what becomes of $\mathbb{Z}$ if we equate 7 to zero.

3.5.2. Why adjoin roots

We now come to one of the most important applications of polynomials to algebra itself: a way to "adjoin" roots of a polynomial to a given commutative ring (i.e., to "create" roots out of thin air).

The classical example for this is the invention of the complex numbers. This idea is somewhat obscured by the fact that nowadays, complex numbers are

usually defined in a down-to-earth, explicit way (viz., as pairs of real numbers[3]) that eschews any use of polynomials[4]. However, this was not always the case. Gerolamo Cardano, back in the 16th century, introduced complex numbers as a tool for solving cubic equations. Specifically, he had a formula (due to Scipione del Ferro) for solving a cubic equation ($ax^3 + bx^2 + cx + d = 0$) that involved square roots. Algebraically, the formula worked well, but quite forbiddingly, a negative number would often appear under these square roots, even though the original cubic equation had three real solutions! It was this vexing situation (and not some abstract curiosity along the lines of "what kind of other numbers could we cook up?") that prompted Cardano to ponder the possibility of imaginary (and thus complex) numbers.

Specifically, Cardano imagined an "imaginary unit" i that satisfies $i^2 = -1$. This new "number" would then entail further "numbers" (by forming sums and products of this "number" with existing real numbers). Since $i^2 = -1$, all these new "numbers" can actually be simplified to the form $a + bi$ with $a, b \in \mathbb{R}$, so it is like an extra degree of freedom is getting added to the real numbers.

Such flights of fancy are often dangerous; after all, one could equally well imagine an "infinite number" ∞ satisfying $0 \cdot \infty = 1$, but this new "number" would cause the number system to collapse (i.e., all numbers to become equal), since it would entail $1 + 1 = 0 \cdot \infty + 0 \cdot \infty = \underbrace{(0+0)}_{=0} \cdot \infty = 0 \cdot \infty = 1$ and therefore $1 = 0$ and so on. There is a good reason why the modern definition of complex numbers (as pairs of real numbers) is preferrable.

3.5.3. How to adjoin roots

Yet, the ability to invent new numbers satisfying desired equalities is a good power to have, and it would be great if we could tell when such an invention is harmless (as opposed to collapsing some of the existing numbers). So let us try to put it on a rigorous footing. What does it mean to introduce a new number?

The simplest case is when we want to introduce a new number x that satisfies no relations (other than the ring axioms). That just means we work in the polynomial ring $\mathbb{R}[x]$. So our "new number" is just the indeterminate of a polynomial ring.

However, in more interesting cases (such as Cardano's), we also want our new number to satisfy some equalities, such as $i^2 = -1$ (in the case of the imaginary unit). The indeterminate x in the ring $\mathbb{R}[x]$ does not satisfy any such equalities (beyond the ones that follow from the ring axioms). But we can use quotient rings to make it satisfy whatever we want! Recall that a quotient ring S/a (where S is a commutative ring and $a \in S$ is an element) is essentially "what becomes of S if we equate a to 0". Thus, if we want our indeterminate x

[3] with addition being entrywise, multiplication being defined by the rule $(a, b)(c, d) = (ac - bd,\ ad + bc)$, and so on

[4] I think this modern definition is due to Hamilton in the 19th century.

to satisfy $x^2 = -1$, then we just have to take the quotient ring $\mathbb{R}[x] / \left(x^2+1\right)$ of our polynomial ring $\mathbb{R}[x]$ (thus equating x^2+1 with 0). The residue class $\overline{x}$ of x in this quotient ring $\mathbb{R}[x] / \left(x^2+1\right)$ will then satisfy $\overline{x}^2 + \overline{1} = \overline{x^2+1} = 0$, so that $\overline{x}^2 = -\overline{1}$, which means that it is an "imaginary unit". So the quotient ring $\mathbb{R}[x] / \left(x^2+1\right)$ is a rigorous interpretation of Cardano's suggestion to introduce a new "number" i satisfying $i^2 = -1$.

This method generalizes to an arbitrary commutative ring R instead of $\mathbb{R}$, and to an arbitrary polynomial $b \in R[x]$. In general, if we start with any commutative ring R and any polynomial $b \in R[x]$, then the quotient ring $R[x]/b$ has an element $\overline{x}$ (the residue class of the polynomial x) that is a root of b (we will give the easy proof of this soon). This quotient ring $R[x]/b$ is not just a ring, but actually a commutative R-algebra (by Theorem 3.4.1 **(b)**); each element $r \in R$ gives rise to an element $\overline{r} \in R[x]/b$ (the residue class of the constant polynomial $r \in R \subseteq R[x]$). As we said, it may happen that some of the existing elements of R "collapse" in this quotient ring $R[x]/b$ (that is, we might have $\overline{r} = \overline{s}$ in $R[x]/b$ for two distinct elements r and s of R), but such "collapses" are natural and cannot be prevented. In the next lecture, we will see a sufficient criterion for when such collapses don't happen.

3.5.4. Some examples

Let us first see some examples of this construction.

As we just said, Cardano's complex numbers are the elements of the quotient ring $\mathbb{R}[x] / \left(x^2+1\right)$, whereas the modern complex numbers are the elements of the ring $\mathbb{C}$ (defined as pairs of real numbers). Let us now show that these two rings are isomorphic (better yet, that these two $\mathbb{C}$-algebras are isomorphic):

Proposition 3.5.2. We have

$$\mathbb{R}[x] / \left(x^2+1\right) \cong \mathbb{C} \qquad \text{as } \mathbb{R}\text{-algebras.}$$

Concretely: There is an $\mathbb{R}$-algebra isomorphism

$$\begin{aligned} \mathbb{R}[x] / \left(x^2+1\right) &\to \mathbb{C}, \\ \overline{p} &\mapsto p[i]. \end{aligned}$$

Proof sketch. Here is a six-step procedure to prove this claim (and, more generally, to prove any claim like this):

1. Give a putative definition of the alleged isomorphism.
2. Prove that this definition actually defines a map (or, to put it colloquially, that "the map is well-defined").

3. Prove that this map is an $\mathbb{R}$-algebra morphism.
4. Prove that this map is injective.
5. Prove that this map is surjective.
6. Conclude that this map is an $\mathbb{R}$-algebra isomorphism (since every invertible $\mathbb{R}$-algebra morphism is an $\mathbb{R}$-algebra isomorphism).

Let us just say a few words about these six steps.

Step 1 has already been done in the statement of Proposition 3.5.2: Our map is defined to be the map

$$\begin{aligned} \mathbb{R}\left[x\right] / \left(x^2+1\right) &\to \mathbb{C}, \\ \overline{p} &\mapsto p\left[i\right]. \end{aligned}$$

For Step 2, we need to prove that if two polynomials $p, q \in \mathbb{R}\left[x\right]$ satisfy $\overline{p} = \overline{q}$, then $p\left[i\right] = q\left[i\right]$. Let us do this. Let $p, q \in \mathbb{R}\left[x\right]$ be two polynomials that satisfy $\overline{p} = \overline{q}$. Then, $p - q \in \left(x^2+1\right)\mathbb{R}\left[x\right]$, so that $p - q = \left(x^2+1\right) r$ for some $r \in \mathbb{R}\left[x\right]$. Consider this r. Substituting i for x in the equality $p - q = \left(x^2+1\right) r$, we obtain

$$p\left[i\right] - q\left[i\right] = \underbrace{\left(i^2+1\right)}_{\substack{=0 \\ (\text{since } i^2=-1)}} r\left[i\right] = 0,$$

so that $p\left[i\right] = q\left[i\right]$. Thus, Step 2 has been completed.

Step 3 is straightforward (since addition, multiplication and scaling on $\mathbb{R}\left[x\right] / \left(x^2+1\right)$ are defined by $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{ab}$ and $r\overline{a} = \overline{ra}$).

Alternatively, Steps 2 and 3 can be handled in one swoop using the universal property of quotient R-algebras (Theorem 3.4.2). This is how I do it in the text (proof of Proposition 4.5.2).

Now we come to Step 4 (injectivity): We need to prove that the map

$$\begin{aligned} \mathbb{R}\left[x\right] / \left(x^2+1\right) &\to \mathbb{C}, \\ \overline{p} &\mapsto p\left[i\right] \end{aligned}$$

is injective. In other words, we need to prove that its kernel is $\{0\}$ (since it is an $\mathbb{R}$-linear map, and we know[5] that a linear map is injective if its kernel is $\{0\}$). In other words, we need to prove that if a polynomial $p \in \mathbb{R}\left[x\right]$ satisfies $p\left[i\right] = 0$, then $\overline{p} = 0$ (that is, p is a multiple of x^2+1).

So let $p \in \mathbb{R}\left[x\right]$ be a polynomial that satisfies $p\left[i\right] = 0$. Let us apply the division-with-remainder theorem for polynomials (Theorem 3.3.8 **(a)** in Lecture 25) to $R = \mathbb{R}$ and $b = x^2+1$ and $a = p$ (we can do this, since the leading

[5] from Lemma 2.4.9 in Lecture 20

coefficient of x^2+1 is a unit). We conclude that there is a **unique** pair (q,r) of polynomials in $\mathbb{R}[x]$ such that

$$p = q \cdot \left(x^2+1\right) + r \qquad \text{and} \qquad \deg r < \deg\left(x^2+1\right).$$

Consider this pair (q,r). From $p = q\cdot\left(x^2+1\right)+r$, we obtain $p-r = q\cdot\left(x^2+1\right) \in \left(x^2+1\right)\cdot\mathbb{R}[x]$, so that $\overline{p} = \overline{r}$ in $\mathbb{R}[x]/\left(x^2+1\right)$. Hence, $p[i] = r[i]$ (by the same argument that we used in Step 2 above, but now with r instead of q). Hence, $r[i] = p[i] = 0$.

From $\deg r < \deg\left(x^2+1\right) = 2$, we see that $\deg r \leq 1$, so that r is a polynomial of degree ≤ 1. In other words, $r = a+bx$ for some $a,b \in \mathbb{R}$. Consider these a,b. Now, our map (whose injectivity we are currently proving) sends $\overline{r}$ to $\underbrace{r}_{=a+bx}[i] = (a+bx)[i] = a+bi$. Thus, we find $a+bi = r[i] = 0$. Therefore, $a=b=0$ (since $a,b\in\mathbb{R}$). Thus, $r=0$ (since $r=a+bx$). Hence, $\overline{p} = \overline{r} = \overline{0} = 0$, as we desired to prove. Thus, we are done with Step 4.

Step 5 is again almost trivial: Every complex number $(a,b) \in \mathbb{C}$ can be written as

$$(a,b) = a+bi = (a+bx)[i],$$

which is the image of the residue class $\overline{a+bx}$ under our map. Thus, our map is surjective.

Finally, Step 6 is automatic: Since our map is injective and surjective, it is bijective, i.e., invertible. But an invertible $\mathbb{R}$-algebra morphism is automatically an $\mathbb{R}$-algebra isomorphism (by a result from §2.9.6 in Lecture 22).

Thus, all six steps have been made, so that Proposition 3.5.2 is proved. □

There are many other results like Proposition 3.5.2, revealing some known and unknown rings as quotients of polynomial rings. Here is a selection (see §4.5.1 in the text for proofs):

Proposition 3.5.3. **(a)** Recall the ring $\mathbb{Z}[i]$ of Gaussian integers. Then,

$$\mathbb{Z}[x]/\left(x^2+1\right) \cong \mathbb{Z}[i] \qquad \text{as } \mathbb{Z}\text{-algebras.}$$

More concretely, the map

$$\begin{aligned} \mathbb{Z}[x]/\left(x^2+1\right) &\to \mathbb{Z}[i], \\ \overline{p} &\mapsto p[i] \end{aligned}$$

is a $\mathbb{Z}$-algebra isomorphism.

(b) Recall the ring $\mathbb{Q}[i]$ of Gaussian rationals. Then,

$$\mathbb{Q}[x]/\left(x^2+1\right) \cong \mathbb{Q}[i] \qquad \text{as } \mathbb{Q}\text{-algebras.}$$

More concretely, the map

$$\begin{aligned} \mathbb{Q}[x] / \left(x^2+1\right) &\to \mathbb{Q}[i], \\ \overline{p} &\mapsto p[i] \end{aligned}$$

is a $\mathbb{Q}$-algebra isomorphism.

(c) Recall the ring $\mathbb{S} = \mathbb{Q}\left[\sqrt{5}\right]$ from §1.1.2 (Lecture 2). Then, the map

$$\begin{aligned} \mathbb{Q}[x] / \left(x^2-5\right) &\to \mathbb{S}, \\ \overline{p} &\mapsto p\left[\sqrt{5}\right] \end{aligned}$$

is a $\mathbb{Q}$-algebra isomorphism.

Proposition 3.5.4. We have

$$\begin{aligned} \mathbb{Q}[x] / \left(x^2-1\right) &\cong \mathbb{Q}[C_2] && \text{(the group algebra of the cyclic group } C_2\text{)} \\ &\cong \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\} && \left(\text{a subring of } \mathbb{Q}^{2\times 2}\right) \\ &\cong \mathbb{Q} \times \mathbb{Q} && \text{(a direct product of two } \mathbb{Q}\text{s)} \end{aligned}$$

as $\mathbb{Q}$-algebras.

In the above examples, the quotient ring has always had the form $R[x]/b$, where b is a non-constant polynomial whose leading coefficient is a unit (actually 1). This has the nice consequence that the resulting ring contains a copy of the original ring R as a subring (although we have yet to prove this in full generality). Let us see what happens if the leading coefficient is not a unit or b is constant:

Proposition 3.5.5. (a) For any integer m, we have $\mathbb{Z}[x]/m \cong (\mathbb{Z}/m)[x]$ as $\mathbb{Z}$-algebras.

(b) The ring $\mathbb{Z}[x]/1$ is trivial.

Proposition 3.5.6. Fix a nonzero integer m. Then,

$$\mathbb{Z}[x] / (mx-1) \cong R_m,$$

where R_m is the ring of m-integers as defined in Exercise 5 of homework set #1. Specifically, there is a $\mathbb{Z}$-algebra isomorphism

$$\begin{aligned} \mathbb{Z}[x] / (mx-1) &\to R_m, \\ \overline{p} &\mapsto p\left[\frac{1}{m}\right]. \end{aligned}$$

(This is not quite trivial.)

Proof. See Proposition 4.5.6 in the text. □

As we already announced, the common thread here is that if you have a commutative ring R and a univariate polynomial $b \in R[x]$, then the quotient ring $R[x]/b$ is like "R with a root of b thrown in". In fact, the residue class $\overline{x} \in R[x]/b$ will be this new root of b. This ring $R[x]/b$ is not always as nice as one might hope. In particular, it can happen that distinct elements of R become equal in $R[x]/b$ (for example, $1 \neq 3$ in $\mathbb{Z}$, but $\overline{1} = \overline{3}$ in $\mathbb{Z}[x]/2$), but often enough this is not the case. When this does not happen, the subset $\{\overline{r} \mid r \in R\}$ of $R[x]/b$ is a subring isomorphic to the original ring R, and thus can be viewed as a "copy of R" inside $R[x]/b$; thus, in this case, we can pretend that $R[x]/b$ contains R as a subring (i.e., we can pretend that $R[x]/b$ is an extension of R).

Cardano was lucky in this sense: The complex numbers he introduced as $\mathbb{R}[x]/\left(x^2+1\right)$ (even if he did not write it this way) were really an extension of the real numbers $\mathbb{R}$; distinct real numbers do not become equal in $\mathbb{R}[x]/\left(x^2+1\right)$. We are not that lucky in Proposition 3.5.5 **(a)** (at least not for $m \neq 0$), and certainly not in Proposition 3.5.5 **(b)**.

Cardano was also lucky that the complex numbers form a field. We are not that lucky in Proposition 3.5.4.

When are we lucky and when are we not? Is there a general criterion for when a quotient ring $R[x]/b$ contains a copy of R (as opposed to making distinct elements of R equal) ? Is there a general criterion for when $R[x]/b$ is a field?[6]

Next time, we will see such criteria, and then we will apply them to a natural question: What finite fields are there? We know the finite fields $\mathbb{Z}/p$ for all primes p. The best way to get other finite fields is to start with $\mathbb{Z}/p$ and to "throw" new "numbers" into them – using the very same $R[x]/b$ construction that Cardano used to define $\mathbb{C}$. The technical term for "throwing in" is "**adjoining**", and so this method is called **root adjunction** (since the new "numbers" we adjoin are roots of given polynomials).

[6]This latter question is best asked if R itself is a field.