# Math 332 Winter 2023, Lecture 28: 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 $R$.

## 3.5. Adjoining roots

### 3.5.5. The general construction

Last time, we introduced a way to "adjoin" a root of a polynomial $b \in R[x]$ to a given commutative ring $R$: We took the quotient ring $R[x]/b$ (where $S/b$ is shorthand for $S/bS$).

In particular,

$$\begin{aligned}
&\mathbb{R}[x] / \left(x^2+1\right) \cong \mathbb{C};\\
&\mathbb{Z}[x] / \left(x^2+1\right) \cong \mathbb{Z}[i];\\
&\mathbb{Q}[x] / \left(x^2+1\right) \cong \mathbb{Q}[i];\\
&\mathbb{Q}[x] / \left(x^2-1\right) \cong \mathbb{Q}[C_2] \cong \mathbb{Q}\times\mathbb{Q} \cong \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\};\\
&\qquad \mathbb{Z}[x]/m \cong (\mathbb{Z}/m)[x] \qquad \text{for } m \text{ integer};\\
&\mathbb{Z}[x] / (mx-1) \cong R_m \qquad \text{for } m \text{ nonzero integer};\\
&\qquad R[x]/1 \cong (\text{zero ring}).
\end{aligned}$$

Some of these rings behave nicer than others. Sometimes the quotient ring $R[x]/b$ contains a copy of the original ring $R$; sometimes it doesn't. Can we give general criteria for what will happen in what case?

We start with a general fact:

**Proposition 3.5.1.** Let $b \in R[x]$ be a polynomial.
**(a)** The projection map

$$\begin{aligned} R[x] &\to R[x]/b, \\ p &\mapsto \overline{p} \end{aligned}$$

is an $R[x]$-algebra morphism, and thus an $R$-algebra morphism.
**(b)** The map[1]

$$\begin{aligned} R &\to R[x]/b, \\ r &\mapsto \overline{r} \end{aligned}$$

is an $R$-algebra morphism.

**(c)** For any $p \in R[x]$, we have $p[\overline{x}] = \overline{p}$ in $R[x]/b$.

**(d)** The element $\overline{x} \in R[x]/b$ is a root of $b$.

*Proof.* Fairly straightforward; see Proposition 4.5.7 in the text. □

So $\overline{x}$ is the root of $b$ that we are pulling out of our hat through this $R[x]/b$ construction. Now, we come to the promised criterion for $R[x]/b$ to contain a copy of $R$:

**Theorem 3.5.2.** Let $m \in \mathbb{N}$. Let $b \in R[x]$ be a polynomial of degree $m$ such that its leading coefficient $[x^m]\, b$ is a unit of $R$. Then:

**(a)** Each element of $R[x]/b$ can be uniquely written in the form

$$a_0\overline{x^0} + a_1\overline{x^1} + \cdots + a_{m-1}\overline{x^{m-1}} \qquad \text{for } a_0, a_1, \ldots, a_{m-1} \in R.$$

**(b)** The $m$ vectors $\overline{x^0}, \overline{x^1}, \ldots, \overline{x^{m-1}}$ form a basis of the $R$-module $R[x]/b$. In particular, this $R$-module is free of rank $m$.

**(c)** Assume that $m > 0$. Then, the $R$-algebra morphism

$$\begin{aligned} R &\to R[x]/b, \\ r &\mapsto \overline{r} \end{aligned}$$

is injective. Therefore, $R$ can be viewed as an $R$-subalgebra of $R[x]/b$ (by identifying each $r \in R$ with its image $\overline{r} \in R[x]/b$).

**(d)** Thus, under the assumption that $m > 0$, there exists a commutative ring that contains $R$ as a subring and that contains a root of $b$.

*Proof.* Again, I refer to the text (Theorem 4.5.9). Part **(a)** is the "hard" part, but really a fairly simple consequence of division-with-remainder for polynomials. Part **(b)** is just a restatement of part **(a)**. Part **(c)** follows from part **(b)** (since $\overline{r} = 0$ would mean $r \cdot \overline{x^0} + 0 \cdot \overline{x^1} + 0 \cdot \overline{x^2} + \cdots + 0 \cdot \overline{x^{m-1}} = 0$, but this would violate linear independence of the basis). Part **(d)** follows from part **(c)**. □

Let us summarize: Generalizing Cardano's construction of $\mathbb{C}$, we have found a way to "adjoin" a (new) root of a given polynomial $b \in R[x]$ to a given commutative ring $R$. The resulting commutative ring $R[x]/b$ is always a commutative $R$-algebra and always contains a root of $b$. When $b$ is non-constant (i.e., has positive degree) and has an invertible leading coefficient, this ring $R[x]/b$ furthermore contains a copy of $R$ as a subring. This conclusion sometimes remains true even if the leading coefficient of $b$ is not invertible (e.g., in

[1] Note the difference between the maps in part **(a)** and in part **(b)**: The map in part **(a)** takes as input a polynomial $p \in R[x]$, whereas the map in part **(b)** takes as input a scalar $r \in R$ (and treats it as a constant polynomial, i.e., as $rx^0 \in R[x]$). If you regard $R$ as a subring of $R[x]$, you can thus view the map in part **(b)** as a restriction of the map in part **(a)**.

our $\mathbb{Z}[x] / (mx-1) \cong R_m$ example for $m \neq 0$), but such claims always require separate proofs.

## 3.6. Field extensions from adjoining roots

So far so good. But when is $R[x]/b$ a field?

First, we restrict ourselves to the case when $R$ is a field (otherwise, it happens very rarely). Accordingly, we will call it $F$ instead of $R$.

We begin with two simple facts about polynomials over a field:

**Proposition 3.6.1.** Let $F$ be a field. Then, the units of the polynomial ring $F[x]$ are the nonzero constant polynomials.

*Proof.* Easy! (See Proposition 4.6.1 in the text.) □

**Proposition 3.6.2.** Let $F$ be a field. Let $b \in F[x]$ be a polynomial. Then, $b$ is irreducible (in the sense of Definition 1.14.13 **(a)** in Lecture 16) if and only if $b$ is an irreducible polynomial in the classical sense (i.e., if $b$ is non-constant and cannot be written as a product of two non-constant polynomials).

*Proof.* Easy! (See Proposition 4.6.2 in the text.) □

There is an easy criterion for polynomials of degree $\leq 3$ to be irreducible:

**Proposition 3.6.3.** Let $F$ be a field. Let $b \in F[x]$ be a polynomial such that $2 \leq \deg b \leq 3$. Then, $b$ is irreducible if and only if $b$ has no root in $F$.

*Proof.* $\Longrightarrow$: Assume that $b$ is irreducible. If $b$ has a root $r$ in $F$, then $x - r \mid b$ in $F[x]$ (by Proposition 3.3.11 in Lecture 26), which entails that $b = (x-r) \cdot q$ for some $q \in F[x]$, and thus $b$ is not irreducible (because degree considerations show that $\deg q = \underbrace{\deg b}_{\geq 2} - 1 \geq 2 - 1 = 1$, so that $q$ is not a unit, and of course $x - r$ is not a unit either). But we assumed that $b$ is irreducible. Thus, $b$ cannot have a root in $F$. The "$\Longrightarrow$" direction of Proposition 3.6.3 is thus proved.

$\Longleftarrow$: Assume that $b$ has no root in $F$. We must show that $b$ is irreducible. In other words, we must prove that $b$ cannot be written as a product of two non-constant polynomials (since $\deg b \geq 2$ shows that $b$ is not constant).

Assume the contrary. Thus, $b = uv$ for two non-constant polynomials $u, v \in F[x]$. Consider these polynomials $u$ and $v$. They satisfy $\deg u \geq 1$ and $\deg v \geq 1$ (since they are non-constant). However, from $b = uv$, we obtain $\deg b = \deg(uv) = \deg u + \deg v$ (by Proposition 3.3.5 **(c)** in Lecture 15, since $F$ is a field and thus an integral domain). If both $\deg u$ and $\deg v$ were $\geq 2$, then this would entail $\deg b = \underbrace{\deg u}_{\geq 2} + \underbrace{\deg v}_{\geq 2} \geq 2 + 2 = 4$, which would contradict $\deg b \leq 3 < 4$. Thus, $\deg u$ and $\deg v$ cannot both be $\geq 2$. Hence, at least one

of $\deg u$ and $\deg v$ is at most 1. We WLOG assume that $\deg u \leq 1$ (otherwise, swap $u$ with $v$). Then, $\deg u = 1$ (since $\deg u \leq 1$ and $\deg u \geq 1$). In other words, $u = \alpha x + \beta$ for some $\alpha, \beta \in F$ with $\alpha \neq 0$. Consider these $\alpha, \beta$. Since $F$ is a field, $\alpha \in F$ is a unit (since $\alpha \neq 0$), so that $-\dfrac{\beta}{\alpha}$ is a well-defined element of $F$. From $u = \alpha x + \beta$, we obtain $u\left[-\dfrac{\beta}{\alpha}\right] = \alpha\left(-\dfrac{\beta}{\alpha}\right) + \beta = 0$. Now, substituting $-\dfrac{\beta}{\alpha}$ for $x$ into $b = uv$, we obtain

$$b\left[-\frac{\beta}{\alpha}\right] = \underbrace{u\left[-\frac{\beta}{\alpha}\right]}_{=0} \cdot v\left[-\frac{\beta}{\alpha}\right] = 0.$$

This shows that $-\dfrac{\beta}{\alpha}$ is a root of $b$. Hence, $b$ has a root in $F$, contradicting our assumption that $b$ has no root in $F$. This contradiction shows that our last assumption was false. This completes the proof of the "$\Longleftarrow$" direction of Proposition 3.6.3. □

Note that Proposition 3.6.3 would fail if $\deg b$ was allowed to be 4. For instance, the degree-4 polynomial $x^4 + 4 \in \mathbb{Q}[x]$ has no roots in $\mathbb{Q}$ (or in $\mathbb{R}$, for that matter), but it is not irreducible[2].

Now we come to the actually crucial result of this section:

**Theorem 3.6.4.** Let $F$ be a field. Let $b \in F[x]$ be a nonzero polynomial. Then, the ring $F[x]/b$ is a field if and only if $b$ is irreducible.

*Proof.* This is the polynomial analogue of the fact that $\mathbb{Z}/n$ is a field (for a given positive integer $n$) if and only if $n$ is prime (part of Corollary 1.6.2 in Lecture 5). Our proof of the latter fact can be adapted to Theorem 3.6.4 (with some changes: most importantly, "the numbers $1, 2, \ldots, n-1$" must be replaced by "the nonzero polynomials of degree $< \deg b$", and we need Bezout's theorem for polynomials instead of Bezout's theorem for integers[3]). Alternatively, you can find the proof of the "$\Longleftarrow$" direction in the text (Theorem 4.6.4), and that is the only direction we will need. □

Here is an instructive example:

- The polynomial $x^2 + \overline{1} \in (\mathbb{Z}/3)[x]$ is irreducible. (This is easily checked using Proposition 3.6.3.)

[2] In fact, $x^4 + 4 = \left(x^2 + 2x + 2\right)\left(x^2 - 2x + 2\right)$.

[3] **Bezout's theorem for polynomials** says that if $a$ and $b$ are two polynomials in $F[x]$, then $\gcd(a, b)$ (more precisely, any gcd of $a$ and $b$) can be written in the form $ua + vb$ for some polynomials $u, v \in F[x]$. This follows easily from the fact that the polynomial ring $F[x]$ is a PID (which, in turn, follows from Theorem 3.3.16 in Lecture 26).

Thus, Theorem 3.6.4 yields that the ring

$$(\mathbb{Z}/3)[x] / \left(x^2 + \overline{1}\right)$$

is a field. Theorem 3.5.2 **(b)** tells us that this field is a free $\mathbb{Z}/3$-module of rank 2 (with basis $\left(\overline{x^0}, \overline{x^1}\right)$). In other words, it is isomorphic to $(\mathbb{Z}/3)^2$ as a $\mathbb{Z}/3$-module. So its size is

$$\left|(\mathbb{Z}/3)^2\right| = 3^2 = 9.$$

Thus, we have found a field with 9 elements. (Aside: This field is also isomorphic to the quotient ring $\mathbb{Z}[i]/3$, so there is a second way to get it. In a sense, this is not surprising: $\mathbb{Z}[i]/3$ is obtained from $\mathbb{Z}$ by first adjoining a square root of $-1$ and then quotienting out all multiples of 3, whereas $(\mathbb{Z}/3)[x] / \left(x^2 + \overline{1}\right)$ is obtained from $\mathbb{Z}$ by first quotienting out all multiples of 3 and then adjoining a square root of $-1$. It stands to reason that the results should be the same both times, although of course this should be rigorously proved.)

# 4. Finite fields

So we have found a field with 9 elements (in addition to all our finite fields $\mathbb{Z}/p$ with $p$ elements for prime numbers $p$). What other finite fields can we find?

A moment of thought reveals that we can find a finite field with $p^2$ elements for any prime $p \equiv 3 \bmod 4$ using the same construction as our 9-element field (since $p \equiv 3 \bmod 4$ entails that $\overline{-1} \in \mathbb{Z}/p$ is not a square[4], and thus the polynomial $x^2 + \overline{1} \in (\mathbb{Z}/p)[x]$ is irreducible[5]). What else can we find?

We can be more flexible and replace our polynomial $x^2 + \overline{1}$ by other degree-2 polynomials. It is not hard to show that for each prime $p$, there exists an irreducible degree-2 polynomial in $(\mathbb{Z}/p)[x]$: Indeed, for $p = 2$, you can take the polynomial $x^2 + x + \overline{1}$. For odd $p$, you can find some element $u$ of $\mathbb{Z}/p$ that is not a square (exercise!), and use the polynomial $x^2 - u$. Thus, you find an irreducible degree-2 polynomial $b \in (\mathbb{Z}/p)[x]$, and then the quotient ring $(\mathbb{Z}/p)[x]/b$ is a finite field with $p^2$ elements. (See Proposition 5.1.1 in the text for the details of this construction.)

Thus we found finite fields of size $p^2$ for any prime $p$. What about other sizes? What about a finite field of size 6 or 8 or 24 ?

[4]This is implicit in the solution to Exercise 1 **(b)** on midterm #2.

[5]again using Proposition 3.6.3

## 4.1. The characteristic of a field

Let us first discuss finite fields whose size is not a prime power (but a number such as 6 or 10). Do such fields exist?

The answer is "no". Each finite field has its "favorite prime", and its size is a power of that prime. This prime is the so-called "characteristic" of the field, and is defined as follows (not just for finite fields):

**Definition 4.1.1.** Let $F$ be a field. The **characteristic** of $F$ is an integer called $\operatorname{char} F$, defined as follows:

- If there exists a positive integer $n$ such that $n \cdot 1_F = 0_F$, then $\operatorname{char} F$ is the **smallest** such $n$.
- If such an $n$ does not exist, then $\operatorname{char} F$ is defined to be 0.

Roughly speaking, $\operatorname{char} F$ is "how often you have to add $1_F$ to itself to circle back to $0_F$" (except that you declare it to be 0 if this never happens). Examples:

- We have $\operatorname{char}(\mathbb{Z}/p) = p$ for any prime $p$.
- Our finite field of size 9 has characteristic 3.
- We have $\operatorname{char}\mathbb{Q} = 0$.

The characteristic of a field $F$ "knows a lot" about $F$. Here is some of that:

**Theorem 4.1.2.** Let $F$ be a field. Let $p = \operatorname{char} F$. Then:
**(a)** We have $pa = 0$ for each $a \in F$.
**(b)** The field $F$ is a $\mathbb{Z}/p$-algebra (with action given by $\overline{n} \cdot a = na$ for all $n \in \mathbb{Z}$ and $a \in F$).
**(c)** The number $p$ is either prime or 0.
**(d)** If $F$ is finite, then $p$ is a prime.
**(e)** If $F$ is finite, then $|F| = p^m$ for some positive integer $m$.
**(f)** If $p$ is a prime, then $F$ contains "a copy of $\mathbb{Z}/p$" (that is, a subring isomorphic to $\mathbb{Z}/p$).
**(g)** If $p = 0$, then $F$ contains "a copy of $\mathbb{Q}$" (that is, a subring isomorphic to $\mathbb{Q}$): namely, the map

$$\begin{aligned} &\mathbb{Q} \to F, \\ &\frac{a}{b} \mapsto \frac{a \cdot 1_F}{b \cdot 1_F} \qquad (\text{for } a, b \in \mathbb{Z} \text{ with } b \neq 0) \end{aligned}$$

is an injective ring morphism.

*Proof.* See Theorem 5.2.2 in the text.

(In a nutshell: Part **(a)** follows from the $pa = \underbrace{p \cdot 1_F}_{=0_F} \cdot a = 0_F \cdot a = 0$ trick. Part **(b)** follows easily using part **(a)** – you just need to show that $na$ depends only on $\overline{n} \in \mathbb{Z}/p$ and not on $n \in \mathbb{Z}$. Part **(c)** uses the fact that $F$ is an integral domain to argue that $\operatorname{char} F$ cannot be composite (e.g., if $\operatorname{char} F$ was 6, then we would have $(2 \cdot 1_F) \cdot (3 \cdot 1_F) = 6 \cdot 1_F = 0_F$, which would lead to $2 \cdot 1_F$ or $3 \cdot 1_F$ being zero, but this would mean that $\operatorname{char} F$ is actually 2 or 3 rather than 6). Part **(d)** follows from a pigeonhole argument or from Lagrange's theorem from group theory. Part **(e)** follows from parts **(b)** and **(d)**, since a $\mathbb{Z}/p$-algebra is always a $\mathbb{Z}/p$-module, and every $\mathbb{Z}/p$-module is free (because $p$ is prime) and thus isomorphic to $(\mathbb{Z}/p)^m$ for some $m \in \mathbb{N}$. Part **(f)** follows easily from part **(b)** and the definition of a characteristic. Part **(g)** is a bit trickier, but will not be used.) □

Parts **(e)** and **(f)** of Theorem 4.1.2 entail that the size of any finite field is a power of a prime (and said prime is the characteristic of the field). Thus, a finite field cannot have size 6 or 10 or 15 for example.

This leaves the question of prime powers. We know that finite fields of sizes $p$ and $p^2$ exist for any prime $p$, but what about $p^3$ or $p^4$ or $p^{29}$ ?

In general, if we have a prime $p$ and a positive integer $m$, and if we know any irreducible polynomial of degree $m$ over $\mathbb{Z}/p$, then we easily obtain a finite field of size $p^m$ (by adjoining a root of this polynomial). But is there such an irreducible polynomial?

Fortunately, such irreducible polynomials do always exist. Proving this is not at all easy, but can be done. Alternatively, there is another way to construct finite fields of any given prime-power size.

Let me just state the result:

**Theorem 4.1.3.** **(a)** For any prime $p$ and any positive integer $m$, there exists a finite field of size $p^m$.

**(b)** Any two finite fields of the same size are isomorphic.

How do these finite fields look like? Theoretically, the answer is clear: Pick an irreducible polynomial $b$ of degree $m$ over $\mathbb{Z}/p$, and adjoin its root to $\mathbb{Z}/p$ (that is, form the quotient ring $(\mathbb{Z}/p)[x]/b$). No explicit formula for such a polynomial is known (except in specific cases like $m = p$). Finding a nice explicit construction of a finite field of size $p^m$ is an open problem! The brute-force approach (try every degree-$m$ polynomial until you find an irreducible one) might sound stupid, but is not too far from the best known algorithm.

*Proof of Theorem 4.1.3.* See the text (§5.2 till §5.4 for part **(a)**; §5.5 for part **(b)**). □

Sadly, our treatment of finite fields has to stop at this strange and unsatisfactory place. More can be found in Chapter 5 of the text, and much more

in dedicated books on the subject, such as [MulMum07] (an introduction) and [LidNie00] (a comprehensive reference).

## References

[LidNie00] Rudolf Lidl, Harald Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications **20**, Cambridge University Press, 2nd edition 1997.

[MulMum07] Gary L. Mullen, Carl Mummert, *Finite Fields and Applications*, Student Mathematical Library **41**, AMS 2007.