POLYNOMIAL MODULAR ARITHMETIC

TIM SMITS

1. The construction of $F[T]/(p(T))$

Our goal is to mimic to construction of $\mathbb{Z}/n\mathbb{Z}$ in the setting of polynomial rings. Throughout this handout, F will denote a field and $p(T)$ a non-constant monic polynomial.

Definition 1.1. Let $p(T) \in F[T]$. Define a relation $\sim_{p(T)}$ on $F[T]$ by $f(T) \sim_{p(T)} g(T)$ if $p(T) \mid f(T) - g(T)$.

Proposition 1. *The relation $\sim_{p(T)}$ is an equivalence relation on $F[T]$.*

Proof. Exercise. □

Definition 1.2. For $p(T) \in F[T]$, define $F[T]/(p(T)) = \{[f(T)] : f(T) \in F[T]\}$, the set of equivalence classes under the relation $\sim_{p(T)}$.

Since we have a division algorithm in $F[T]$, we know that for any $f(T) \in F[T]$, that $f(T) = p(T)q(T) + r(T)$ for some unique $r(T) \in F[T]$ with $r(T) = 0$ or $\deg(r) < \deg(p)$. This means $f(T) \sim_{p(T)} r(T)$. Then as a set, $F[T]/(p(T))$ consists of equivalence classes of the possible remainders, that is, $[f(T)]$ where $\deg(f) < \deg(p)$.

Example 1.3. Let $p(T) = T^2 + T + 1$ in $(\mathbb{Z}/2\mathbb{Z})[T]$. Then $(\mathbb{Z}/2\mathbb{Z})[T]/(T^2 + T + 1) = \{[0], [1], [T], [T + 1]\}$.

Example 1.4. Let $p(T) = T^2 + 1$ in $\mathbb{R}[T]$. Then $\mathbb{R}[T]/(T^2 + 1) = \{[a + bT] : a, b \in \mathbb{R}\}$.

Note that the previous example highlights one of the major differences between $\mathbb{Z}/n\mathbb{Z}$ and $F[T]/(p(T))$: the first set is *finite*, while the latter need not be. Indeed, we see that the only way $F[T]/(p(T))$ can be finite is if F is finite, since $F[T]/(p(T))$ always contains elements of the form $[a]$ for $a \in F$.

The same story that happens for the integers mod n also happens for $F[T]$ mod $p(T)$:

Definition 1.5. Define addition and multiplication operations on $F[T]/(p(T))$ by $[f(T)] + [g(T)] = [f(T) + g(T)]$ and $[f(T)] \cdot [g(T)] = [f(T)g(T)]$.

Proposition 2. *The operations of addition and multiplication above make $F[T]/(p(T))$ into a commutative ring with additive identity $[0]$ and multiplicative identity $[1]$.*

Proof. Left as an exercise – very similar to the proof in $\mathbb{Z}/n\mathbb{Z}$. □

Like before, we'll often write $f(T) \equiv g(T) \bmod p(T)$ to mean that $f(T) \sim_{p(T)} g(T)$, or equivalently, that $[f(T)] = [g(T)]$ in $F[T]/(p(T))$. Arithmetic in this ring plays out very much like how arithmetic in $\mathbb{Z}/n\mathbb{Z}$ works out.

Example 1.6. In $(\mathbb{Z}/2\mathbb{Z})[T]/(T^2+T+1)$, we have $[T^2+T+1]=[0]$, so solving for $[T^2]$ says $[T^2]=[T+1]$, i.e. $T^2 \equiv T+1 \bmod T^2+T+1$. If we compute some other powers of $[T]$, we find $T^3 = T\cdot T^2 \equiv T^2+T \equiv 1 \bmod T^2+T+1$, and $T^4=(T^2)^2 \equiv (T+1)^2 \equiv T^2+1 \equiv (T+1)+1 \equiv T \bmod T^2+T+1$.

Example 1.7. $(\mathbb{Z}/3\mathbb{Z})[T]/(T^2+1)$ has 9 elements: the equivalence classes $[a+bT]$ with $a,b \in \mathbb{Z}/3\mathbb{Z}$. Since $[T^2+1]=[0]$, this tells us that $[T^2]=[2]$. We have $(2T+1)+(T+2) \equiv 0 \bmod T^2+1$, and $(2T+1)(T+2)=2T^2+5T+2 \equiv 2T \bmod T^2+1$.

Example 1.8. In $\mathbb{Q}[T]/(T^2-1)$, we have $[T^2-1]=[0]$. Since $T^2-1=(T+1)(T-1)$, this means $[(T+1)][(T-1)]=[0]$, so that $\mathbb{Q}[T]/(T^2-1)$ is **not** an integral domain.

2. The structure of $F[T]/(p(T))$

Positive integers in $\mathbb{Z}$ are analogous to monic polynomials in $F[T]$, and primes in $\mathbb{Z}$ are analogous to monic irreducibles in $F[T]$. Like in the integers, the structure will depend on if $p(T)$ is irreducible or not.

Theorem 2.1. *$[f(T)] \in F[T]/(p(T))$ is a unit if and only if $(f(T),p(T))=1$ in $F[T]$.*

Proof. The proof is basically identical to how it worked in $\mathbb{Z}/n\mathbb{Z}$: suppose that $[f(T)] \in F[T]/(p(T))$ is a unit, so there is $[g(T)] \in F[T]/(p(T))$ such that $[f(T)][g(T)]=[1]$. This means that $f(T)g(T) \equiv 1 \bmod p(T)$, so there is $h(T) \in F[T]$ such that $f(T)g(T)=1+p(T)h(T)$. This says that $f(T)g(T)-p(T)h(T)=1$, so that $(f(T),p(T))=1$. Conversely, suppose that $(f(T),p(T))=1$. By Bezout's lemma, there are polynomials $g(T),h(T) \in F[T]$ such that $f(T)g(T)+p(T)h(T)=1$. Taking this equation mod $p(T)$ says that $f(T)g(T) \equiv 1 \bmod p(T)$, i.e. that $[f(T)][g(T)]=[1]$. This says that $[f(T)]$ has multiplicative inverse $[g(T)]$, so it's a unit. □

Corollary 2.2. *$F[T]/(p(T))$ is a field if and only if $p(T)$ is irreducible in $F[T]$.*

Proof. Any element of $F[T]/(p(T))$ is of the form $[f(T)]$ for some polynomial $f(T)$ of degree strictly smaller than that of $p(T)$. If $p(T)$ is irreducible, we must have that $(f(T),p(T))=1$ for any non-zero $f(T)$ for degree reasons. This means that $[f(T)]$ is invertible in $F[T]/(p(T))$. If $p(T)$ is reducible, we may write $p(T)=f(T)g(T)$ for some non-constant $f(T),g(T) \in F[T]$. This says that $[f(T)][g(T)]=[0]$ in $F[T]/(p(T))$, so that $[f(T)]$ is a zero divisor. Since fields have no zero divisors, this means that $F[T]/(p(T))$ is not a field. □

Example 2.3. Since $(T+2,T^2-1)=1$ in $\mathbb{Q}[T]$, we have that $[T+2]$ is invertible in $\mathbb{Q}[T]/(T^2-1)$. To find a multiplicative inverse, we first find a $\mathbb{Q}[T]$-linear combination of $T+2$ and T^2-1 that gives 1. By the division algorithm, we have $T^2-1=(T+2)(T-2)+3$, so $\frac{1}{3}(T^2-1)+(T+2)(\frac{1}{3}(2-T))=1$. Taking this mod T^2-1 says that $[T+2]^{-1}=[\frac{1}{3}(2-T)]$.

Example 2.4. Since T^2+T+1 is irreducible in $(\mathbb{Z}/2\mathbb{Z})[T]$, the ring $(\mathbb{Z}/2\mathbb{Z})[T]/(T^2+T+1)$ is actually a field. The elements in this field are $[0],[1],[T],[T+1]$, and $[T]^{-1}=[T+1]$ because $[T]\cdot[T+1]=[T^2+T]=[1]$.

3. field extensions

The above result tells us that modding out by irreducible polynomials in $F[T]$ lets us construct new fields. We start with a motivating example.

Example 3.1. Since T^2+1 is irreducible in $\mathbb{R}[T]$, $\mathbb{R}[T]/(T^2+1)$ is a field. There is a natural inclusion map $\iota : \mathbb{R} \to \mathbb{R}[T]/(T^2+1)$ given by $a \to [a]$ for any $a \in \mathbb{R}$. This map is an injective field homomorphism, so $\mathrm{Im}(\iota)$ is an isomorphic copy of $\mathbb{R}$ living inside of $\mathbb{R}[T]/(T^2+1)$. Since $[T^2] = [-1]$, this says that $[T]$ is a solution to the equation x^2+1 in $\mathbb{R}[T]/(T^2+1)$, i.e. this is a field containing the real numbers that also contains a square root of -1. At this point, one might "recognize" $\mathbb{R}[T]/(T^2+1)$ as $\mathbb{C}$ (in fact, one might take this as the definition of $\mathbb{C}$!)

Explicitly, I claim that the map $f : \mathbb{C} \to \mathbb{R}[T]/(T^2+1)$ given by $f(a+bi) = [a+bT]$ is a field isomorphism. Note that $f(1) = [1]$. For $z = a+bi$ and $w = c+di \in \mathbb{C}$, we have $f(z+w) = f((a+c)+(b+d)i) = [(a+c)+(b+d)T] = [a+bT]+[c+dT] = f(z)+f(w)$. Similarly, we have $f(zw) = f((ac-bd)+(ad+bc)i) = [(ac-bd)+(ad+bc)T] = [ac+(ad+bc)T+bdT^2] = [a+bT][c+dT] = f(z)f(w)$. This says that f is a field homomorphism. The map is clearly surjective, since $[a+bT]$ is mapped to by $a+bi$, and from homework 4, field homomorphisms are automatically injective. Therefore, f is an isomorphism.

Definition 3.2. Let F be a field. We call a field K a **field extension** of F if K contains a subfield that's isomorphic to F.

Example 3.3. We showed above that $\mathbb{R}[T]/(T^2+1)$ is a field extension of $\mathbb{R}$ that's isomorphic to $\mathbb{C}$.

Given a field F, we can always construct a field extension of F that contains solutions to polynomial equations.

Theorem 3.4. *Let $p(T)$ be an irreducible polynomial. Then $F[T]/(p(T))$ is a field extension of F where $p(T)$ has a root.*

Proof. Let $\iota : F \to F[T]/(p(T))$ be the natural inclusion map defined by $a \to [a]$ for $a \in F$. Then ι is an injective field homomorphism, so $\mathrm{Im}(\iota) \cong F$ is a subfield of $F[T]/(p(T))$, meaning $F[T]/(p(T))$ is a field extension of F. We now show that $p(T)$ has a root in $F[T]/(p(T))$. Write $p(T) = T^n + \ldots + a_0$. We have $[0] = [T^n + \ldots + a_0] = [T]^n + \ldots + [a_0]$. This says that $\alpha = [T]$ is a root of of the polynomial $T^n + \ldots + a_0$ in $F[T]/(p(T))$ as desired. □

Corollary 3.5. *Let $p(T) \in F[T]$ be a non-constant polynomial. Then there is a field extension K of F such that K contains a root of $p(T)$.*

Proof. Let $\pi(T)$ be an irreducible factor of $p(T)$ in $F[T]$. Then by the above, $K = F[T]/(\pi(T))$ is a field extension of F where $\pi(T)$ has a root α. Since $\pi(T) \mid p(T)$, this means that $p(\alpha) = 0$ in K, so that $p(T)$ has a root in K. □

Definition 3.6. Let K be a field extension of F, and let $\alpha \in K$. The smallest subfield of K that contains both F and α is denoted as $F(\alpha)$, and is called the **extension of F generated by α**.

Theorem 3.7. *Let $p(T) \in F[T]$ be an irreducible polynomial. Let K be a field extension of F where $p(T)$ has a root α. Then $F(\alpha) \cong F[T]/(p(T))$.*

Proof. Consider the evaluation at α map $ev_\alpha : F[T]/(p(T)) \to F(\alpha)$ defined by $e_\alpha([p(T)]) = p(\alpha)$. I claim that this is a field isomorphism. First, we should check that this map is well defined. If $[f(T)] = [g(T)]$ in $F[T]/(p(T))$, this means that $f(T) = g(T) + p(T)h(T)$ for some $h(T) \in F[T]$. In K, we then have that $f(\alpha) = g(\alpha) + p(\alpha)h(\alpha) = g(\alpha)$ because α is a root of $p(T)$ in K. This says that ev_α is well defined. It's quite easy to see that ev_α is

a field homomorphism. We get injectiveness for free, because ev_α is a field homomorphism, so $F[T]/(p(T)) \cong \mathrm{Im}(ev_\alpha)$ is a subfield of K. Since $F \subset \mathrm{Im}(ev_\alpha)$ and $\alpha \in \mathrm{Im}(ev_\alpha)$ (it's the image of T), as $F(\alpha)$ is the *smallest* subfield of K with this property, we must have $\mathrm{Im}(ev_\alpha) = F(\alpha)$, so that ev_α is surjective and therefore an isomorphism. □

Note that this theorem says that *any* field extension of F where $p(T)$ has a root contains a copy of $F[T]/(p(T))$ and that up to isomorphism, this is the *smallest* such subfield with this property.

Example 3.8. Let $p(T) = T^2 + T + 1$ and write $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$. Then $\mathbb{F}_2[T]/(T^2 + T + 1)$ is a field extension of $\mathbb{F}_2$ where $p(T)$ has a root, which we'll denote as α, and we can write $\mathbb{F}_2[T]/(T^2 + T + 1) \cong \mathbb{F}_2(\alpha)$. From our earlier example, we know the elements of $\mathbb{F}_2(\alpha)$ are $0, 1, \alpha, \alpha + 1$. The two roots of $T^2 + T + 1$ in $\mathbb{F}_2(\alpha)$ are given by α and $\alpha + 1$.

Example 3.9. The polynomial $T^2 - 2$ is irreducible in $\mathbb{Q}[T]$, because $\sqrt{2}$ is not rational. In $\mathbb{R}$, we have that $\sqrt{2}$ is a root of $p(T)$, so $\mathbb{Q}[T]/(T^2 - 2) \cong \mathbb{Q}(\sqrt{2})$, given by the map $[f(T)] \to f(\sqrt{2})$. Since elements of $\mathbb{Q}[T]/(T^2 - 2)$ are of the form $[a + bT]$ for some $a, b \in \mathbb{Q}$, this says that as a set, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, which is consistent with how we defined this before.

Note that $-\sqrt{2}$ is *also* a root of $T^2 - 2$ in $\mathbb{R}$, so we also have $\mathbb{Q}(-\sqrt{2}) \cong \mathbb{Q}[T]/(T^2 - 2)$. This says that $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(-\sqrt{2})$. In otherwords, the roots of an irreducible polynomial are *algebraically indistinguishable*, in the sense that the field constructed by adjoining any root gives the same field extension. The way one differentiates between $\sqrt{2}$ and $-\sqrt{2}$ in $\mathbb{R}$ is that one is positive and one is negative, using the extra structure of the ordering of real numbers.

Example 3.10. The polynomial $p(T) = T^3 - 3T^2 + 3T - 3$ is irreducible in $\mathbb{Q}[T]$ by Eisenstein's criterion. Let α be a root of $p(T)$ in $\mathbb{R}$. Then $\mathbb{Q}(\alpha) \cong \mathbb{Q}[T]/(T^3 - 3T^2 + 3T - 3)$. As a set, we have $\mathbb{Q}[T]/(T^3 - 3T^2 + 3T - 3) = \{a + bT + cT^2 : a, b, c \in \mathbb{Q}\}$ so elements of $\mathbb{Q}(\alpha)$ are of the form $a + b\alpha + c\alpha^2$ with $a, b, c \in \mathbb{Q}$. How does the arithmetic in $\mathbb{Q}(\alpha)$ work?

Let's say we wanted to find the multiplicative inverse of $1+\alpha+\alpha^2 \in \mathbb{Q}(\alpha)$. We can do this as follows: passing through the isomorphism of $\mathbb{Q}[T]/(T^3-3T^2+3T-3)$ and $\mathbb{Q}(\alpha)$, this says we're trying to find the inverse of $[1+T+T^2]$ in $\mathbb{Q}[T]/(T^3-3T^2+3T-3)$, which is equivalent to finding polynomials $f(T), g(T) \in \mathbb{Q}[T]$ such that $(1+T+T^2)f(T)+(T^3-3T^2+3T-3)g(T) = 1$. Using WolframAlpha, one finds that $(1+T+T^2)(\frac{1}{31}(6T^2-19T+16))+(T^3-3T^2+3T-3)(\frac{1}{31}(-6T-5)) = 1$, so the inverse of $[1 + T + T^2]$ is $[\frac{1}{31}(6T^2 - 19T + 16)]$. Passing back through the isomorphism, this says that $\frac{1}{1+\alpha+\alpha^2}$ in $\mathbb{Q}(\alpha)$ is given by $\frac{1}{31}(6\alpha^2 - 19\alpha + 16)$.