26 Finite Fields

26.1 Splitting Fields

Last time, we stated the uniqueness of the splitting field of a polynomial.

Proposition 26.1
If F is a field, and P a (not necessarily irreducible) polynomial in F, then there exists a *unique* extension E/F up to isomorphism, such that P splits as a product of linear factors in $E[x]$ as $P(x) = \prod(x - \alpha_i)$, and $E = F(\alpha_1, \ldots, \alpha_n)$.

Proof. The idea of the proof is fairly easy — we essentially add in roots one by one, which immediately proves existence. Uniqueness follows from uniqueness in adjoining a root of an irreducible polynomial (since adjoining any root is equivalent to adjoining an abstract one).

First, we'll prove existence by induction on the degree of P. Let P_1 be an irreducible factor of P, and let $F_1 = F[x]/(P_1)$, which (as we've seen earlier) is essentially the construction of adjoining a root of P_1 to F. Then in $F_1[x]$, P factors as $P(x) = (x - \alpha)Q(x)$, where α is a root of P_1.

Now let E be the splitting field for Q over F_1 (which exists by the induction assumption). Then we claim E is also a splitting field for P over F. This follows directly from the definition — suppose $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of P. Then P splits completely in $E[x]$. But we also have $E = F_1(\alpha_2, \ldots, \alpha_n)$, and since $F_1 = F(\alpha_1)$, then $E = F(\alpha_1, \ldots, \alpha_n)$.

So we've proved existence of the splitting field. To prove uniqueness, we again use induction. Suppose that E' is another splitting field; we'll construct an isomorphism between E' and E.

First, we can find a root α' of P_1 in E'. Then if we set $F_1' = F(\alpha') \subset E'$, we know that $F(\alpha') \cong F(\alpha)$, since both are isomorphic to the abstract construction $F[x]/(P)$.

This isomorphism between $F(\alpha)$ and $F(\alpha')$ sends $\alpha \mapsto \alpha'$. Suppose it sends $Q \in F_1[x]$ to $Q' \in F_1'[x]$, so we have $P = (x - \alpha')Q'$ (the isomorphism fixes F, and therefore P). Now E' is a splitting field for Q' over F_1'. So uniqueness of the splitting field of Q (which we know by the induction assumption) implies that the isomorphism between F_1 and F_1' extends to an isomorphism between E and E', and the two splitting fields are isomorphic. $\square$

We'll see more proofs similar to this last idea later, where we construct isomorphisms between field extensions.

Student Question. *What happens if P has repeated roots?*

Answer. *In this case, it doesn't matter — for instance, the splitting field of P^2 is the same as that of P.*

26.2 Construction of Finite Fields

We'll now turn to *finite* fields. First notice that if F is a finite field, it can't contain $\mathbb{Q}$ (since $\mathbb{Q}$ is infinite), so it must contain $\mathbb{F}_p$ — we saw last class that every field contains $\mathbb{Q}$ or $\mathbb{F}_p$ for some prime p. Moreover, since F is finite as a set, the extension $F/\mathbb{F}_p$ is also finite, so F is finite-dimensional as a $\mathbb{F}_p$-vector space. Let $n = [F : \mathbb{F}_p] = \dim_{\mathbb{F}_p} F$. Then we must have $|F| = p^n$ — if we choose a basis for F (forgetting we can multiply elements, and only using the vector space structure), this identifies F with $\mathbb{F}_p^n$ (n-tuples of elements in $\mathbb{F}_p$, corresponding to the coordinates in this basis), which has p^n elements.

This was a fairly straightforward observation, but the converse is also true!

Theorem 26.2
For every prime p and every $n \geq 1$, there exists a field of $q = p^n$ elements. Furthermore, any two such fields are isomorphic.

As a result, we have a unique field of $q = p^n$ elements, which we denote by $\mathbb{F}_q$. Note that except when $n = 1$, the field $\mathbb{F}_q$ is very different from $\mathbb{Z}/q\mathbb{Z}$ (which is not a field). They're not even isomorphic as additive groups! (For example, $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, but $\mathbb{F}_4$ and $\mathbb{Z}/4\mathbb{Z}$ have very different structure.)

One way to construct a field of q elements would be to find an irreducible polynomial of degree n in $\mathbb{F}_p[x]$ (and quotient by that polynomial). This is easy to do when n is small — for example, if $p = 4k+3$, the polynomial x^2+1 is irreducible, so

$$\mathbb{F}_{p^2} = \mathbb{F}_p[x]/(x^2+1).$$

Similarly, we have

$$\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1).$$

But this is harder for general n — it's possible to prove one always exists via a counting argument (counting all polynomials, and all ways to produce a product of lower-degree polynomials), but this won't be the approach we use.

Instead, we'll use a sort of "magic trick" — we'll consider the *Artin–Schreier polynomial* $A(x) = x^q - x$.

Lemma 26.3

Let F be any field containing $\mathbb{F}_p$, and let $q = p^n$. Then the set of roots of A in F,

$$\{x \in F \mid x^q - x = 0\},$$

is a subfield of F.

This is quite exceptional! Usually, to construct a field from a polynomial, we adjoin roots and then take all possible sums and products. But in this case, when we take all roots, the result is actually *closed* under arithmetic operations — and we don't need to do anything more.

Proof. We must check that for $\alpha, \beta \in F$ with $A(\alpha) = 0$ and $A(\beta) = 0$, we have:

(1) $A(\alpha\beta) = 0$,

(2) $A(\beta^{-1}) = 0$ (if $\beta \neq 0$), and

(3) $A(\alpha+\beta) = 0$.

The first two are straightforward (and would work if we replaced q with *any* exponent) — for (1), since $\alpha^q = \alpha$ and $\beta^q = \beta$, we have $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$. We can check (2) similarly.

Now for (3), note that in any ring containing $\mathbb{F}_p$, we have

$$(x+y)^p = x^p = y^p.$$

This follows from the Binomial Theorem, since $\binom{p}{i} \equiv 0 \pmod{p}$ for $i = 1, \ldots, p-1$ — if we write $\binom{p}{i} = p!/i!(p-i)!$, the numerator is divisible by p and the denominator is not. Now using induction, we see that $(x+y)^q = x^q + y^q$ if $q = p^n$ for any n. So $\alpha^q = \alpha$ and $\beta^q = \beta$ implies that

$$(\alpha+\beta)^q = \alpha^q + \beta^q = \alpha + \beta,$$

and thus $A(\alpha+\beta) = 0$. $\square$

With this tool, we can now prove Theorem 26.2.

Proof of Theorem 26.2. We'll first prove uniqueness. Suppose that F is a field of $q = p^n$ elements. Now consider the multiplicative group $F^\times$ (the group of all nonzero elements of F under multiplication). This has $q-1$ elements, so the order of any element of $F^\times$ must divide $q-1$; therefore $\alpha^{q-1} = 1$ for all $\alpha \neq 0$. Then $\alpha^q = \alpha$ for *all* $\alpha \in F$ (since this is true for 0 as well). So $A(\alpha) = 0$ for all $\alpha \in F$.

But now we have a polynomial of degree q, which has q roots in F. The only way this happens is if the polynomial splits completely — we have that $x - \alpha \mid A(x)$ for all $\alpha \in F$, so by unique factorization in $F[x]$, the product of all terms $x - \alpha$ must divide $A(x)$ as well, and since $\deg(A(x)) = q$ (and both sides are monic), we must then have

$$A(x) = \prod_{\alpha \in F}(x - \alpha).$$

But then F is a splitting field of A over $\mathbb{F}_p$, and the uniqueness of F follows from the uniqueness of the splitting field.

To prove existence, we can simply let F be the splitting field of A over $\mathbb{F}_p$; we then need to check that $|F| = q$.

First, by Lemma 26.3, we have $A(\alpha) = 0$ for all $\alpha \in F$ — we know that F is *generated* by the roots of A, but the lemma implies that these roots are closed under arithmetic operations, so *all* elements of F are roots of A.

So then the number of elements in F is the number of roots of A (which splits completely in F). In particular, we immediately see that $|F| \le \deg A = q$. To see that equality holds, it suffices to check that A has no multiple roots.

To check this, we use derivatives — in real or complex analysis, we know that a function has a higher-order root at a if a is also a root of the derivative. Of course, here we're in a much more abstract setting, and we can't define derivatives using limits. However, we can still use this idea, by using *formal derivatives* — the formal derivative of a polynomial $P(x) = a_n x^n + \cdots + a_0$ is the familiar formula $P'(x) = na_n x^{n-1} + \cdots + a_1$. It's easy to check that the formulas $(P+Q)' = P' + Q'$ and $(PQ)' = PQ' + P'Q$ still hold. Now, if P has a multiple root at α, then $P(x) = (x-\alpha)^2 Q(x)$ for some Q, which means

$$P'(x) = 2(x-\alpha)Q(x) + (x-\alpha)^2 Q'(x)$$

also has a root at α. So it's still true that a multiple root of P is also a root of its derivative. In particular, if $\gcd(P, P') = 1$, then P has no multiple roots (in any field containing its field of coefficients).

But it's easy to compute the derivative of A — we have $A'(x) = (x^q - x)' = qx^{q-1} - 1$. But q is 0 in F (since F has characteristic p)! So $A'(x)$ is just -1, and $\gcd(A, A') = 1$. So A has no multiple roots, which means $|F| = q$. □

Once we have this construction, we can then derive concrete information about irreducible polynomials.

26.3 Structure of Finite Fields

There's more that we can say about the structure of $\mathbb{F}_q$.

Proposition 26.4
The multiplicative group $\mathbb{F}_q^\times$ is cyclic, and is therefore isomorphic to $\mathbb{Z}/(q-1)\mathbb{Z}$.

Proof. Since $\mathbb{F}_q^\times$ is a finite abelian group, it's isomorphic to $\prod \mathbb{Z}/p_i^{d_i}\mathbb{Z}$ for some d_i. By the Chinese Remainder Theorem, it's enough to show that each prime p appears at most once in this decomposition.

But assume for contradiction that some prime p appears twice (here p is used to denote any prime, not the characteristic of $\mathbb{F}_q$). Then there's at least p^2 elements of order dividing p, meaning that $\alpha^p = 1$ (since the group $\mathbb{Z}/p^d\mathbb{Z}$ contains p elements of order dividing p, so we can take one such element from each copy and elements of order 1 from the remaining terms in the product). But then the polynomial $x^p - 1$ would have p^2 roots; this is impossible, since a polynomial of degree p can have at most p roots. □

MIT OpenCourseWare
https://ocw.mit.edu

Resource: Algebra II Student Notes
Spring 2022
Instructor: Roman Bezrukavnikov
Notes taken by Sanjana Das and Jakin Ng

For information about citing these materials or our Terms of Use, visit: https://ocw.mit.edu/terms.