FEBRUARY 20 NOTES

1. 13.5: Separable and Inseparable Extensions

Definition 1.1. A polynomial F is called **separable** if it has no multiple roots. It is called **inseparable** if it has multiple roots.

Last time we ended with:

Theorem 1.2. *Every irreducible polynomial over a field of characteristic* 0 *is separable. Even in characteristic* p*, if* $D_x p(x)$ *is non-zero, the same proof applies to show irreducible polynomials are separable. In particular, the only way to find inseparable irreducible polynomials is to have those whose derivative is identically* 0*.*

Let's discuss polynomials in characteristic p.

Proposition 1.3. *Let* F *be a field of characteristic* p*. Then, for any* $a, b \in F$*,*

$$(a+b)^p = a^p + b^p \quad \text{and} \quad (ab)^p = a^p b^p.$$

Proof. The equation $(ab)^p = a^p b^p$ holds in any field by commutativity. We must only verify the first, which we do using the Binomial Theorem:

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i$$

where

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

are integers. Because $p!$ is divisible by p and for $0 < i < p$, no term in the denominator is a multiple of p, the integer $\binom{p}{i}$ is a multiple of p. Therefore, every term other than $i = 0$ or $i = p$ is zero over a field of characteristic p¡ so we have

$$(a+b)^p = a^p + b^p.$$

□

Remark 1.4. Let F be a field of characteristic p. By the previous proposition, the function $\phi : F \to F$ given by $\phi(a) = a^p$ is an injective endomorphism. This is a very important function called the **Frobenius map**.

Corollary 1.5. If $\mathbb{F}$ is a finite field of characteristic p, then every element of $\mathbb{F}$ is a pth power.

Proof. Because the Frobenius map $\mathbb{F} \to \mathbb{F}$ sending a to a^p is injective and $\mathbb{F}$ is finite, it is also surjective. □

What does this tell us? Suppose $p(x) \in F[x]$ is an inseparable irreducible polynomial over a field F of characteristic p. To be inseparable, the derivative must be identically 0, i.e. $D_x p(x) = 0$, which is possible if and only if each exponent in the polynomial $p(x)$ is a multiple of p. In other words,

$$p(x) = a_m x^{mp} + a_{m-1} x^{(m-1)p} + \cdots + a_1 x^p + a_0$$

so $p(x) = q(x^p)$ for the polynomial $q(x)$ given by

$$q(x) = a_m x^m + a_{m-1} x^{(m-1)} + \cdots + a_1 x + a_0.$$

If F is a finite field, by the previous corollary, each element $a_i \in F$ is also a pth power, so we could write each coefficient a_i as b_i^p for some $b_i \in F$. Therefore,

$$\begin{aligned} p(x) &= b_m^p x^{mp} + b_{m-1}^p x^{(m-1)p} + \cdots + b_1^p x^p + b_0^p \\ &= (b_m x^m)^p + \cdots + (b_1 x)^p + b_0^p \\ &= (b_m x^m + \cdots + b_1 x + b_0)^p \end{aligned}$$

so $p(x)$ is the pth power of another polynomial, which is impossible if $p(x)$ is irreducible. Therefore, we have just shown the following:

Proposition 1.6. *Every irreducible polynomial over a finite field $\mathbb{F}$ is separable.*

Definition 1.7. A field K is called **perfect** if $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) = p$ and every element $k \in K$ is a pth power.

With this definition in hand, we've actually shown:

Proposition 1.8. *Every irreducible polynomial over a perfect field is separable.*

Going back to the inseparable polynomial, we showed that if $p(x)$ is inseparable, then $p(x) = p_1(x^p)$ for some polynomial $p_1(x)$. If $p_1(x)$ is inseparable, then $p_1(x) = p_2(x^p)$ for some $p_2(x)$ (and hence $p(x) = p_2(x^{p^2})$), and so on. This must eventually end with a separable polynomial $p_k(x)$ whose derivative is not identically zero because polynomials have finite degree. Therefore, for any inseparable polynomial, we have the following:

Proposition 1.9. *Let $p(x)$ be an irreducible polynomial over a field F of characteristic p. There is a unique integer $k \geq 0$ such that $p(x) = p_{sep}(x^{p^k})$ where $p_{sep}(x) \in F[x]$ is a separable irreducible polynomial. The integer p^k is called the* ***inseparable*** *degree of $p(x)$, denoted $\deg_i p(x)$, and the degree of the separable polynomial $p_{sep}(x)$ is called the* ***separable*** *degree of $p(x)$, denoted $\deg_s p(x)$. These satisfy the relationship*

$$\deg p(x) = \deg_i p(x) \deg_s p(x).$$

Example 1.10. The polynomial $p(x) = x^2 - t$ over $\mathbb{F}_2(t)$ has $p_{sep}(x) = x - t$, so has separable degree 1 and inseparable degree 2.

Definition 1.11. A field K is **separable** over R if every element of K is the root of a separable polynomial over F.

We will discuss separable extensions more in the future!

We end with some commentary on finite fields.

Let $n > 0$ be any positive integer and consider the splitting field of the polynomial $x^{p^n} - x$ over $\mathbb{F}_p$. This polynomial is separable, so has p^n distinct roots. Note first that *every* element of $\mathbb{F}_p$ is a root of this polynomial: by Fermat's Little Theorem, for every $a \in \mathbb{F}_p$, $a^p \equiv a \pmod{p}$, so $a^{p^n} - a = 0$ in $\mathbb{F}_p$.

Also, α and β are any two roots, then $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$. We also have: $(\alpha\beta)^{p^n} = \alpha\beta$; $(\alpha^{-1})^{p^n} = \alpha^{-1}$; and $(\alpha+\beta)^{p^n} = \alpha + \beta$. Therefore, the p^n roots of $x^{p^n} - x$ form a field, which is subfield of the splitting field that contains $\mathbb{F}_p$. The splitting field was defined to be the *smallest* subfield containing all of the roots, so this implies that the splitting field is exactly equal to the set of p^n roots of this polynomial. Therefore, for any $n > 0$, we have just constructed a finite field F of order p^n such that $[F : \mathbb{F}_p] = n$. In other words, for any $n > 0$, there exist finite extensions of $\mathbb{F}_p$ of degree n. We denote this field by $\mathbb{F}_{p^n}$.

Perhaps miraculously, these are *all* of the possible finite fields. Let F be any finite field of characteristic p, which by definition contains its prime subfield $\mathbb{F}_p$. If F has degree n over $\mathbb{F}_p$, then $|F| = p^n$. Because F is a field, $F^\times$ is a group of order $p^n - 1$, so, by Lagrange's Theorem, $\alpha^{p^n-1} = 1$ for every $\alpha \in F^\times$. In other words, every $\alpha \in F$ is a root of the polynomial $x^{p^n} - x$ over $\mathbb{F}_p$, so F

is contained in a splitting field for this polynomial. But, $|F| = p^n$ and the splitting field has p^n elements, so in fact F must be equal to the splitting field for this polynomial.

In summary: any finite field has order p^n for some prime number p and integer n, and up to isomorphism, the only finite fields are $\mathbb{F}_p$ and $\mathbb{F}_{p^n}$, the splitting field of the polynomial $x^{p^n} - x$ over $\mathbb{F}_p$.

2. 13.6: Cyclotomic Polynomials and Extensions

For the remainder of today's class, we will revisit the cyclotomic fields $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity satisfying the equation $x^n - 1 = 0$.

Definition 2.1. For $n \geq 1$, the **group of nth roots of unity** is denoted $\mu_n = \{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}\}$. We've already seen that $\mu_n \cong \mathbb{Z}_n$.

Note that, if $d \mid n$, then for any $\zeta \in \mu_d$, $1 = \zeta^d$ so $\zeta^n = (\zeta^d)^{n/d}) = 1$, so $\zeta \in \mu_n$. In other words, $\mu_d \subset \mu_n$. Conversely, if $\zeta \in \mu_n$ and $\zeta^d = 1$ is the smallest power of ζ satisfying $\zeta^d = 1$, then because $\operatorname{ord}(\zeta) \mid n$, we must have $d \mid n$.

Definition 2.2. The nth cyclotomic polynomial $\Phi_n(x)$ is the polynomial whose roots are the primitive nth roots of unity:

$$\Phi_n(x) = \Pi_{\zeta \in \mu_n \text{ primitive}}(x - \zeta) = \Pi_{1 \leq a < n, \gcd(a,n)=1}(x - \zeta_n^a).$$

Note $\deg \Phi_n = \phi(n)$.

By definition, we know

$$x^n - 1 = \Pi_{\zeta \in \mu_n}(x - \zeta)$$

and we could group the roots by order. Using that $\operatorname{ord}(\zeta) = d$ if and only if $d \mid n$ and ζ is a primitive dth roots of unity, we can write the polynomial as:

$$x^n - 1 = \Pi_{d|n}\Pi_{\zeta \in \mu_d \text{ primitive}}(x - \zeta) = \Pi_{d|n}\Phi_d(x).$$

This allows us to compute $\Phi_n(x)$ recursively! For example, by definition, $\Phi_1(x) = x - 1$ and $\Phi_2(x) = x + 1$. Then, we compute higher n:

$$x^3 - 1 = \Phi_1(x)\Phi_3(x) = (x - 1)\Phi_3(x)$$

so we can solve and find $\Phi_3(x) = x^2 + x + 1$.

$$x^4 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x) = (x - 1)(x + 1)\Phi_4(x)$$

so we can solve and find $\Phi_4(x) = x^2 + 1$.

In general, for p prime, we have $x^p - 1 = \Phi_1(x)\Phi_p(x) = (x - 1)\Phi_p(x)$ which yields

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

The behavior of $\Phi_n(x)$ is always similar to this:

Lemma 2.3. *The polynomial $\Phi_n(x)$ is a monic irreducible polynomial in $\mathbb{Z}[x]$ of degree $\phi(n)$, and hence the minimal polynomial of ζ_n for any primitive nth root of unity.*

Proof. It is clear from the definition that $\Phi_n(x)$ is monic and of degree $\phi(n)$. Now, we verify that $\Phi_n(x) \in \mathbb{Z}[x]$ by induction: the base case $n = 1$ is clear, so assume $n > 1$ and $\Phi_d(x) \in \mathbb{Z}[x]$ for all $d < n$. By definition, $x^n - 1 = f(x)\Phi_n(x)$ where $f(x) = \Pi_{d|n, d \leq n}\Phi_d x$. By the division algorithm, because $f(x)$ and $x^n - 1 \in \mathbb{Q}[x]$, we have $\Phi_n(x) \in \mathbb{Q}[x]$. If $\Phi_n(x)$ were not in $\mathbb{Z}[x]$, we could multiply both sides of

$$x^n - 1 = f(x)\Phi_n(x)$$

by the least common multiple m of the denominators of coefficients in $\Phi_n(x)$. Let $\Phi'(x) = m\Phi_n(x)$. By construction, for any prime $p \mid m$, we have $\Phi'(x) \neq 0 \pmod{p}$ (we multiplied by the least common multiple of the denominators, so if a_i was the coefficient of Φ_n in which the highest power of p appeared in the denominator, ma_i would not be divisible by p). This gives

$$m(x^n - 1) = f(x)\Phi'(x)$$

but, for any $p \mid m$, this says $f(x)\Phi'(x) = 0 \in \mathbb{Z}_p[x]$, and as $\Phi'(x) \neq 0$, this implies $f(x) = 0$. In other words, $f(x)$ is divisible by p for every prime p dividing m. However, $f(x)$ is monic, so cannot be divisible by any constant other than 1, which gives a contradiction. Therefore, $\Phi_n(x) \in \mathbb{Z}[x]$.

Next, we verify the irreducibility. Suppose not, so $\Phi_n(x) = f(x)g(x)$ for $f, g \in \mathbb{Z}[x]$ monic polynomials, and assume that $f(x)$ is irreducible. Let ζ be a primitive nth root of unity that is a factor of $f(x)$, which implies that $f(x)$ is the minimal polynomial for ζ. Then, for any prime p such that p does not divide n, ζ^p is also a primitive nth root of unity, so ζ^p must be a root of f or g. If it were a root of g, then $g(\zeta^p) = 0$, and as f was the minimal polynomial of ζ, $f(x)$ must divide $g(x^p) \in \mathbb{Z}[x]$, i.e. $g(x^p) = f(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Mod p, using that $g(x^p) = (g(x))^p$ in $\mathbb{F}_p[x]$ (recall: every coefficient satisfies $a_i^p = a_i$ by Fermat's Little Theorem), we have $(g(x))^p = f(x)h(x) \in \mathbb{F}_p[x]$ which is a UFD, so $f(x)$ and $g(x)$ have some common factor in $\mathbb{F}_p[x]$. Therefore, $\Phi_n(x) = f(x)g(x)$ has a multiple root in $\mathbb{F}_p[x]$ (the root of the common factor). This is a contradiction: there are n distinct roots of unity over any field of characteristic not dividing n.

Therefore, ζ^p must be a root of $f(x)$ for every p not dividing n, which implies that for any a relatively prime to n, $a = p_1 \dots p_k$ where $p_i \nmid n$, and $\zeta^a = ((\zeta^{p_1})^{p_2}) \dots^{p_k}$ is a root of $f(x)$. In other words, every primitive nth root of unity is a root of $f(x)$, which implies $f(x) = \Phi_n(x)$ is irreducible. $\square$

By construction, this implies:

Corollary 2.4. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.