Lecture 1-10: Multiple roots and separability

January 10, 2025

I noted last time that I have not quite proved that a field of order p^n exists for all prime powers p^n, since I need to verify that the polynomial $x^{p^n} - x$ does not have multiple roots in its splitting field. More generally, I make the following

Definition, p. 546

A nonconstant polynomial q over a field K is *separable* (over K) if q does not have multiple roots in its splitting field. An algebraic element x of an extension L of K is called separable over K if it satisfies a separable polynomial over K. We say that L is separable over K if all of its elements are.

How can you tell whether a polynomial is separable without constructing its splitting field? The answer unexpectedly comes from calculus. I first define the derivative q' of a polynomial $q = \sum_{i=0}^{n} q_i x^i \in K[x]$ to be $\sum_{i=1}^{n} i q_i x^{i-1} \in K[x]$, as in Math 124; this definition does not require the notion of a limit. The sum, difference, and product rules for polynomials then carry over from calculus and show that if q has a root α in any extension field with multiplicity at least two, so that $(x-\alpha)^2$ divides q in this field, then $x-\alpha$ divides q' and q, q' have a nontrivial common factor. The Euclidean algorithm shows that if q and q' have a common factor in $L[x]$ for some extension L of K, then they have a common factor already in $K[x]$.

Now specialize down to the case of greatest interest, where $q \in K[x]$ is irreducible. Then q and q' cannot have a common divisor, *unless* $q' = 0$. This certainly cannot happen if the characteristic of K is 0; in general we have $q' = 0$ if and only if the characteristic of K is $p > 0$ and q is a polynomial in x^p. We conclude that

Corollary 34, p. 547

Every irreducible polynomial q over a field K of characteristic 0 is separable. The same holds in characteristic $p > 0$, provided that q is not a polynomial in x^p.

The polynomial $q = x^{p^n} - x \in F_p[x]$ is almost a polynomial in x^p, but not quite; since its derivative is -1, it has no multiple roots in its splitting field, so that this splitting field has order exactly p^n. Thus a field F_1 of order $q = p^n$ exists for every prime power p^n and F_q is unique up to isomorphism (Proposition 15, p. 586). We also see that F_{p^m} is a subfield of F_{p^n} if and only if m divides n, as mentioned earlier.

Over a field K of characteristic p one has the "freshman's dream" $(a+b)^p = a^p + b^p$, since by the binomial theorem $(a+b)^p = \sum_{i=0}^{n} \binom{p}{i} a^i b^{p-i}$ an p divides every binomial coefficient $\binom{p}{i}$ for $0 < i < p$. Since we obviously have $(ab)^p = a^p b^p$ for all $a, b \in K$ and $x^p = 0$ if and only if $x = 0$ it follows that

Definition, p. 549

The *Frobenius map* sending x to x^p is an isomorphism of any field K of characteristic $p > 0$ into itself.

Given a nonconstant polynomial $q(x^p) \in K[x]$, this polynomial factors over its splitting field L first as $(x^p - r_1) \dots (x^p - r_m)$ for some $r_i \in L$ and then as $(x - s_1)^p \dots (x - s_m)^p$ for some $s_i \in L$ with $s_i^p = r_i$. Thus whenever separability fails for a polynomial q, it does so spectacularly: *every* root of q in its splitting field has multiplicity a multiple of p. Note also that every element in a finite field F of characteristic p has a unique pth root (Corollary 36, p. 549), since the Frobenius map must be an isomorphism of F onto itself in this case.

I showed last time that the coefficients of the cyclotomic polynomial $\Phi_m[x]$ lie in $\mathbb{Z}$; In fact they are usually ± 1; it is not until n reaches 105 (the product of the first three odd primes) that coefficients other than ± 1 and 0 appear in Φ_n. I now specialize down to the case where $K = \mathbb{Q}$.

Theorem 41, p. 554

The polynomial Φ_n is irreducible in $\mathbb{Q}[x]$ for all n.

Proof.

By Gauss's Lemma, it is enough to show that Φ_n is irreducible in $\mathbb{Z}[x]$. Suppose contrarily that Φ_n factors nontrivially as $g(x)h(x)$, where $g, h \in \mathbb{Z}[x]$ are monic and g is irreducible. As every positive integer less than n and relatively prime to it is a product of primes not dividing n, there would have to be a primitive nth root α and a prime p not dividing n such that α is a root of g while α^p is a root of h. Then $h(x^p)$ also has α as a root; by the irreducibility of g we have $g(x)|h(x^p)$ in $\mathbb{Z}[x]$. Reducing all coefficients mod p we get that the reduction $\overline{g}(x)$ divides $\overline{h}(x^p) = (\overline{h}(x))^p$ in $\mathbb{Z}_p[x]$, whence $\overline{g}\overline{h} = \overline{\Phi}_n(x)$ and $\overline{x^n - 1}$ all have multiple roots in an extension of $\mathbb{Z}_p$. This is absurd, as the derivative nx^{n-1} of $x^n - 1$ is nonzero in $\mathbb{Z}_p(x)$ and has 0 as its only root. □

This proof was historically one of the first applications of methods in characteristic p to prove a result in characteristic 0. We now know that the degree of $e^{2\pi i/n} \in \mathbb{C}$ is $\phi(n)$ over $\mathbb{Q}$, where ϕ is the Euler phi-function. I should mention that although the reduction of $\overline{\Phi}_n$ modulo any prime q makes sense and the reduction $\overline{x^n - 1}$ of $x^n - 1$ is again the product of the $\overline{\Phi}_d$ as d runs over the divisors of n it is *not* generally true that $\overline{\Phi}_n$ is irreducible in $\mathbb{Z}_q$; the above proof depends heavily on unique factorization in $\mathbb{Z}$.

Returning to the constructibility of the regular n-gon we now see that the regular n-gon is not constructible with straightedge and compass unless n is a power of 2 times product of distinct Fermat primes, as suggested by earlier results.

Returning to splitting fields we note that the degree of the splitting field of a polynomial is in general quite difficult to compute. For example, consider the polynomial $q = x^8 - 2 \in \mathbb{Q}[x]$. This polynomial is irreducible, by the Eisenstein Criterion, so the degree of its splitting field over $\mathbb{Q}$ is a multiple of 8. If α is the unique real positive root of q, then all of its roots in $\mathbb{C}$ are obtained by multiplying α by an 8th root of 1. A primitive 8th root of 1 in $\mathbb{C}$ is $e^{\pi i/4} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ and $\sqrt{2} = \alpha^4$ lies already in $\mathbb{Q}(\alpha)$. Thus one obtains a splitting field of q by passing from $K = \mathbb{Q}(\alpha)$ to $K' = K(i)$; this is a proper extension since K lies in the real field $\mathbb{R}$ while K' does not. The upshot is that the splitting field K' has degree 16 over $\mathbb{Q}$.

On the other hand, the splitting field L of the very similar polynomial $r = x^8 - 3 \in \mathbb{Q}[x]$ has degree 32 over $\mathbb{Q}$. We get to L from $\mathbb{Q}(\beta)$, β the real positive root of r, by adjoining first $\sqrt{2}$ and then i, each of these adjunctions multiplying the degree by 2. It is a bit tricky to prove that $\sqrt{2} \notin \mathbb{Q}(\beta)$.

Next time we will bring groups into the picture, by looking at automorphisms of field extensions; these are called Galois groups. They turn out to have the "right" order (equal to the degree of the extension) precisely when the extension is the splitting field of a separable polynomial.