September 7:

Math 432 Class Lecture Notes

- Uniqueness of Splitting Fields
- The Fundamental Theorem of Algebra

0.1 Uniqueness of Splitting Fields

Earlier we saw that there was a splitting field for any polynomial. We now prove uniqueness. Curiously, it turns out that we have to state and prove a slightly stronger result, for the sake of making an induction argument go smoothly.

Theorem 1. If $\phi\colon F \to \tilde{F}$ is a field isomorphism and E and $\tilde{E}$ are splitting fields of polynomials $f \in F[x]$ and $\tilde{f} \in \tilde{F}[x]$, respectively, then there exists an isomorphism $\Phi\colon E \to \tilde{E}$ such that $\Phi(x) = \phi(x)$ for all x in F.

Proof: By induction on $[E : F]$. If $[E : F] = 1$, then $E = F$ and $\tilde{E} = \tilde{F}$, so ϕ itself is the desired mapping.

Assume that the theorem is true for any extension of fields of degree less than n. Let $p(x)$ be an irreducible factor of $f(x)$, let α be a zero of $p(x)$ in E, and let β be a zero of $\phi(p(x))$ in $\tilde{E}$.

By the Uniqueness of Root Fields Theorem, there exists an isomorphism Φ_1 from $F(\alpha)$ to $\tilde{F}(\beta)$ that agrees with ϕ on F and carries α to β.

So $f(x) = (x - \alpha)g(x)$ for some $g(x) \in F(\alpha)[x]$. Then E is a splitting field for $g(x)$ over $F(\alpha)$ and $\tilde{E}$ is a splitting field for $\phi_1(g(x))$ over $\tilde{F}(\beta)$. The degree of g is less than the degree of f, so $[E : F(a)] < [E : F] = n$ and thus, by the induction assumption, there exists an isomorphism Φ from E to $\tilde{E}$ that agrees with Φ_1 on $F(\alpha)$ and therefore with ϕ on F.

0.2 Fundamental Theorem of Algebra

There is a surprisingly simple proof of the Fundamental Theorem of Algebras that uses the existence of splitting fields, the theorem on symmetric polynomials proved last time, the fact that square roots exist in the complex numbers, and the fact that a polynomial of odd degree with real coefficients has a real root.

More precisely, we prove:

Theorem 2. Any polynomial of positive degree in $\mathbf{C}[x]$ has a root in $\mathbf{C}$.

From this one easily deduces that any polynomial in $\mathbf{C}[x]$ factors into linear factors, i.e., that $\mathbf{C}$ is a splitting field for any $f \in \mathbf{C}[x]$, i.e., that $\mathbf{C}$ is "'algebraically closed."

Proof. Let f be a polynomial of degree $n > 0$. Without loss of generality, we can assume that f has real coefficients; indeed, the polynomial $f\overline{f}$ has real coefficients, and if it has a complex root then so does f.

Write the degree n as a power of 2 times an odd number: $n = 2^e m$. We prove that a polynomial f with real coefficients has a complex root by induction on e.

The base case is $e = 0$, i.e., the degree n is odd. In this case the result is well-known from the Intermediate Value Theorem in calculus: for large positive and negative x, $f(x)$ has opposite signs, and is hence zero somewhere in between.

Now assume that $e > 0$ and that the result is true for all real polynomials whose degree has a smaller power of 2 than 2^e.

Choose a splitting field E for f over the real numbers, so that

$$f(t) = a_0 \prod_{i=1}^{n} (t - \alpha_i)$$

for $a_0 \in \mathbf{R}$ and $\alpha_i \in E$. For a real number λ consider the polynomial

$$g(t) = \prod_{i<j} (t - \alpha_i - \alpha_j - \lambda \alpha_i \alpha_j).$$

The product is over all pairs of roots of f, so the degree of g is

$$\frac{n(n-1)}{2} = 2^{e-1} m(n-1).$$

The coefficients of g are symmetric functions of the α_i and, by the symmetric functions theorem, are polynomials in the elementary symmetric functions of the α_i and are therefore real numbers.

By our induction assumption, we know that g has a complex root! Thus for every λ there is a pair i, j such that

$$\alpha_i + \alpha_j + \lambda\alpha_i\alpha_j \quad \in \quad \mathbf{C}.$$

Since there are infinitely many λ and only finitely many pairs i, j it follows that there are distinct λ, λ' that give rise to the same pair. From the previous equation and the equation

$$\alpha_i + \alpha_j + \lambda'\alpha_i\alpha_j \quad \in \quad \mathbf{C}.$$

we deduce that $\alpha_i\alpha_j \in \mathbf{C}$ (subtract the equations and divide by $\lambda - \lambda'$). It follows by subtracting the real number $\lambda\alpha_i\alpha_j$ that $\alpha_i + \alpha_j$ is complex.

Therefore the polynomial

$$(t - \alpha_i)(t - \alpha_j) = t^2 - (\alpha_1 + \alpha_2)t + \alpha_1\alpha_2$$

has complex coefficients. By the quadratic formula it has a root in $\mathbf{C}$ and we are finished. □