September 12:

Math 432 Class Lecture Notes

- Finite fields
- Automorphisms of fields
- Separable Extensions

0.1 Finite fields

The proof of the cyclicity of F^* for finite F was finished — see the class notes from September 10 for details. This enables us to answer several questions about finite fields.

Suppose that F is a finite field. Then we know that the number of elements in F is a power of a prime, say $q = p^n$, so that $[F : \mathbf{F}_p] = n$.

The multiplicative group F^* has order $q - 1$ so every nonzero element u of F satisfies $u^{q-1} = 1$ and it follows that every element of F satisfies $u^q = u$. The polynomial $x^q - x$ has q roots in F, and therefore F is a splitting field for this polynomial.

Since splitting fields exist are unique, we see that there is a finite field with q elements and that it is unique up to isomorphism.

If u is a generator of the cyclic group F^* then $F = \mathbf{F}_p(u)$. The minimal polynomial for u has degree n, and this proves that there is an irreducible polynomial in $\mathbf{F}_p$ of degree n.

Remark 1. With a little more work, one can show that $x^q - x$ is the product of all irreducible polynomials in $\mathbf{F}_p[x]$ whose degree divides n.

Example 2. Over $\mathbf{F}_2$,

$$x^4 - x = x^4 + x = x(x+1)(x^2+x+1)$$

so there are two irreducible polynomials of degree 1 and one of degree 2. Therefore the polynomial x^{16} must factor as

$$x^{16} + x = x(x+1)(x^2+x+1)f(x)g(x)h(x)$$

where f, g, and h are irreducible of degree 4. A little work shows that those irreducible quartics are x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$.

0.2 Automorphisms of fields

If E is an extension of F define

$$\mathrm{Aut}_F(E) := \{\sigma : E \to E \quad | \quad \sigma(x) = x \forall x \in F\}.$$

Example 3. If $F = \mathbf{Q}$ and $E = \mathbf{Q}(i)$ then

$$\mathrm{Aut}_F(E) = \{1, \text{complex conjugation}\}.$$

Example 4. If $F = \mathbf{Q}$ and $E = \mathbf{Q}(\sqrt[3]{2})$ then $\mathrm{Aut}(E) = \{1\}$. Indeed, any automorphism maps a root of $x^3 - 2$ to a root of the same polynomial, and there is a unique root of that polynomial in E.

This is an instance of a general "lifting" result that comes up over and over again.

Theorem 5. If $\phi\colon F \to F'$ is an isomorphism of fields, $f(x) \in F[x]$, E is a root field of F, f' is the polynomial obtained by applying ϕ to each coefficient of f, then any lifting of ϕ to a mapping from E to an extension field E' of F' must map α to a root of f'. Thus there are at most $\deg(f)$ such extensions.

The proof of the theorem is immediate. If $E = F(\alpha)$, and

$$f(\alpha) = \sum a_i \alpha^i = 0$$

then applying an extension Φ to this equation gives

$$\sum \phi(a_i)\Phi(\alpha)^i = f'(\Phi(\alpha)) = 0.$$

Thus the proof of the theorem is shorter than the statement.

(And, as seen in class, the diagram is even shorter.)

0.3 Separable Extensions

From the above general fact, it is clear that the number of embeddings from a root field $F(\alpha)$ into an extension E of F depends on how many roots the minimal polynomial of α has in E. An important technical point comes up: does the polynomial have distinct roots in its splitting field?

Definition 6. A polynomial $f \in F[x]$ is **separable** if its roots are distinct in its splitting field. An element of an extension field is separable over F if its minimal polynomial is separable. An extension field is separable if and only if all of its elements are separable.

In characteristic 0, or over finite fields, any irreducible polynomial, and hence any element and any extension, is separable.

Theorem 7. If F is finite or has characteristic 0, then any irreducible polynomial is separable.

If f has a multiple root then $(x-\alpha)^2$ divides f, and hence $x-\alpha$ divides f'. Thus f and f' have a common factor, which is impossible if f is irreducible and the characteristic is 0 (so that the degree of f' is one less than the degree of f). Conversely, any root α of the gcd of f and f' gives a double factor of f.

Example 8. If $F = \mathbf{F}_p(t)$ is the field of rational functions $r(t)/s(t)$ in an indeterminate t, then the root α of the polynomial $f(x) = x^p - t$ in a root field $F(\alpha)$ is not separable. Indeed, f is irreducible, and is therefore the minimal polynomial of α, but

$$x^p - t = (x - \alpha)^p$$

so that the root field is the splitting field, and the minimal polynomial has repeated roots.

One shows that any inseparable polynomial in characteristic p has the shape $f(x) = g(x^p)$, so that $f' = 0$. If the field is finite, where the Frobenius automorphism is surjective, then $g(x^p) = h(x)^p$ for a suitable h, so that if f is inseparable then it is not irreducible.

An easy argument using the "lifting" principle in the preceding section shows that if E is a splitting field over F then

$$\#\mathrm{Aut}_F(E) \leq [E : F] \, .$$

With more work, one can show that this is also true for any finite extension E/F of fields.

Definition 9. A finite extension E/F is a **galois** extension if equality holds, i.e., if

$$\#\mathrm{Aut}_F(E) = [E : F] .$$

By using the lifting theorem one can show that this holds if E is the splitting field of a separable polynomial. A nontrivial result from galois theory says that in fact any galois extension has the form.

Theorem 10. If E/F is a galois extension then E is the splitting field of a separable polynomial $f \in F[x]$.