Algebra II: Galois Theory (cont.)

We've seen Galois groups of cyclotomic fields.
We've also seen another key example:

$\mathbb{F}_{p^n}/\mathbb{F}_p$ is always Galois, with gp. $\mathbb{Z}/n\mathbb{Z}$, generated by the Frobenius elt $\mathrm{Frob}_p : a \mapsto a^p$.

By the fundamental theorem, $\forall d|n$, $\exists!$ subfield fixed by $\langle \mathrm{Frob}_p^d \rangle$, which is $\cong \mathbb{F}_{p^d}$.

Ex: x^4+1 is irreducible over $\mathbb{Z}$.
But mod p it is reducible $\forall$ primes p.
Indeed, $x^4+1 \equiv (x+1)^4 \pmod 2$, and
for odd p, $8 \mid (p^2-1)$ (easy check)
$\Rightarrow x^4+1 \mid (x^4-1)(x^4+1) = x^8-1 \mid x^{p^2-1}-1 \mid x^{p^2}-x$
$\Rightarrow$ roots of x^4+1 are roots of $x^{p^2}-x$,
and these roots in turn are the elts of $\mathbb{F}_{p^2}$.
Thus, adjoining a root of x^4+1 to $\mathbb{F}_p$ gives an extn of degree at most 2, so x^4+1 is reducible over $\mathbb{F}_p$.

Ex) Finite fields are always simple, as $\mathbb{F}_{p^n}^\times$ is cyclic over $\mathbb{F}_p$. In particular, $\forall n \geq 1$, $\exists$ irred. poly/$\mathbb{F}_p$ of deg. n.
How do we find polys. generating these extns?

Well, we constructed $\mathbb{F}_{p^n}$ as $\mathrm{Split}_{\mathbb{F}_p}(x^{p^n}-x)$,

So if ϑ is a generator $\mathbb{F}_{p^n} = \mathbb{F}_p(\vartheta)$, then $\min\text{poly}(\vartheta) \mid x^{p^n}-x$, and it also has degree n.

Thus, Now, if $f(x)$ is irred. of degree d, $f(x) \mid x^{p^n}-x$,

Then $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}$ is a subfield of degree d $\forall$ roots α of $f(x)$.

Thus, By the Galois structure of finite fields, $d \mid n$ and $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ is Galois $\Rightarrow$ normal $\Rightarrow$ $f(x)$ splits over $\mathbb{F}_p(\alpha)$.

Thus, $x^{p^n}-x$ ~~$=$~~ is the product of all irred. polys over $\mathbb{F}_p$ of degrees $d \mid n$.

To see how to use this to construct finite fields, consider a few examples in characteristic $\neq 2$:

$p=2$, $n=2$: $x^4-x = x(x^3-1) = x(x-1)(x^2+x+1)$ ← the only irred. quadratic

$n=3$: $x^8-x = x(x^7-1) = x(x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$.

$n=4$: $x^{16}-x$

$= x(x-1)(x^2+x+1)(x^{12}+x^9+x^6+x^3+1)$

$= x(x-1)(x^2+x+1)(x^3+x+1)(x^3+x^2+1)$

($d=1$, $d=2$ from above; the irred. quartics cut into:)

$= x(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1)$

This gives us ways of quickly finding explicit reps$^{\text{ns}}$ of finite fields.

For instance, $\mathbb{F}_4 \cong \mathbb{F}_2[x]/(x^2+x+1)$

$\mathbb{F}_8 \cong \mathbb{F}_2[x]/(x^3+x+1) \cong \mathbb{F}_2[x]/(x^3+x^2+1)$

$\mathbb{F}_{16} \cong \mathbb{F}_2[x]/(x^4+x+1) \cong \mathbb{F}_2[x]/(x^4+x^3+1)$ ... etc.

We can even go one step further ... and construct all of the irred. polys of a given degree.

ic fact from # theory: Möbius fn: $\mu(n) := \begin{cases} 1 & n=1 \\ (-1)^r & n = \text{prod. of } r \text{ distinct primes} \\ 0 & \text{else.} \end{cases}$

Th^m (Möbius inversion) [Proof not important to us here.]
If $f: \mathbb{N} \to \mathbb{C}$, and $F(n) = \sum_{d|n} f(d)$, then
$f(n) = \sum_{d|n} \mu(d) F(n/d)$.

Then if $\varphi(n) = \#$ irred. polys of deg. n / $\mathbb{F}_p$,
$p^n = \sum_{d|n} d \cdot \varphi(d) \underset{\text{Möbius}}{\Rightarrow} \varphi(n) = \frac{1}{n} \cdot \sum_{d|n} \mu(d) p^{n/d}$.

(recursive alg. above shows (look at degrees))

Finally, one more cool fact:
Since $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \Leftrightarrow m \mid n$, any two f. fields $\mathbb{F}_{p^{n_1}}, \mathbb{F}_{p^{n_2}}$ are contained in $\mathbb{F}_{p^{n_1 n_2}}$ $\Rightarrow$ we can consider the union of all char. p finite fields which contains all finite extns of $\mathbb{F}_p$ $\Rightarrow$ an alg. closure is $\overline{\mathbb{F}}_p = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$.

Some more properties of Galois gps.

Theorem: If K/F is Galois, $F \subseteq F'$, then KF'/F' is Galois with $\mathrm{Gal}(KF'/F') \cong \mathrm{Gal}(K/K \cap F')$.

Pf: K/F Galois $\Rightarrow$ separable + normal $\Rightarrow K = \mathrm{Split}_F(f(x))$, $f(x)$ separable.
Then KF'/F' is Galois simply because $KF'/F' = \mathrm{Split}_{F'}(f(x))$.
Now K/F Galois $\Rightarrow K/F$ normal ($\Rightarrow$ embeddings of K fixing F are automorphisms of K) $\Rightarrow$ restriction $\varphi: \mathrm{Gal}(KF'/F') \to \mathrm{Gal}(K/F)$, $\sigma \mapsto \sigma|_K$ is well-defined.

This is also a homomorphism, and

$$\ker(\varphi) = \{\sigma \in \mathrm{Gal}(KF'/F') \mid \sigma|_K = 1\}$$

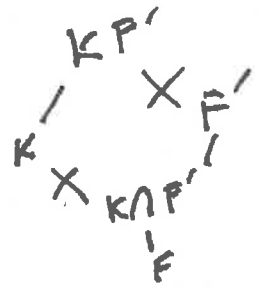
But elts of this kernel are trivial on K and F' (as in $\mathrm{Gal}(KF'/F')$) $\Rightarrow$ trivial on composite $KF' \Rightarrow \ker(\varphi) = 1 \Rightarrow \varphi$ is injective.

Now if $H = \mathrm{Im}(\varphi)$, then all elts of H fix F'. Also the composite $K_H F'$ is fixed by $\mathrm{Gal}(KF'/F')$ $\Rightarrow K_H \supseteq K \cap F'$. Since elts of $\mathrm{Gal}(\cdot/F')$ fix F' and act on $K_H \subseteq K$ by restriction $\sigma|_K \in H$ which fixes H by def^n.

Thus, the fundamental theorem implies $K_H F' = F'$

$\Rightarrow K_H \subseteq F'$. Thus, $K_H \subseteq K \cap F' \Rightarrow K_H = K \cap F'$

$\Rightarrow$ (Fund. Th^m) $H = \mathrm{Gal}(K/K \cap F')$. ☐



Cor: K/F Galois, F'/F finite $\Rightarrow [KF' : F] = \dfrac{[K:F][F':F]}{[K \cap F' : F]}$.

Pf: Immediate from $[KF' : F'] = [K : K \cap F']$ by Th^m.

Th^m: K_1, K_2 both Galois $/F$. Then $K_1 \cap K_2 / F$ is Galois and so is $K_1 K_2$.

$\mathrm{Gal}(K_1K_2/F) \cong \{(\sigma, \tau) \mid \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\} \subseteq \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$

Pf: If $f(x) \in F[x]$ is irreducible, with root $\alpha \in K_1 \cap K_2$, then $\alpha \in K_1$ and K_1/F Galois $\Rightarrow$ all roots of $f(x) \in K_1$. Similarly for K_2, so all roots of $\alpha \in K_1 \cap K_2 \Rightarrow K_1 \cap K_2 / F$ is normal, and it's still separable, so it's Galois.

To study the composite, say $K_1 = \mathrm{Split}_F(f_1(x))$, $K_2 = \mathrm{Split}_F(f_2(x))$

- composite K_1K_2 contains the roots of both $f_1(x), f_2(x)$
if $f_1(x)$ has roots $\alpha_1, \dots, \alpha_n$, $f_2(x)$ has roots $\beta_1, \dots, \beta_m$,
and so K_1K_2, the smallest field containing K_1, K_2, is
$F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) \Rightarrow K_1K_2 = \text{Split}_F(f_1(x)f_2(x))$
$\Rightarrow K_1K_2$ Galois over F. Consider the homomorphism:

$\varphi: \text{Gal}(K_1K_2/F) \to \text{Gal}(K_1/F) \times \text{Gal}(K_2/F)$
$\sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$

Elts. of the kernel are trivial on $K_1, K_2 \Rightarrow$ on K_1K_2
$\Rightarrow$ trivial kernel $\Rightarrow \varphi$ is injective.

Now since $(\sigma|_{K_1})|_{K_1\cap K_2} = \sigma|_{K_1\cap K_2} = (\sigma|_{K_2})|_{K_1\cap K_2}$,
the image is contained in the subgroup in the theorem
statement, call it H. We proceed by computing $|H|$.
For every $\sigma \in \text{Gal}(K_1/F)$, there are $|\text{Gal}(K_2/K_1\cap K_2)|$
elts. $\tau \in \text{Gal}(K_2/F)$ whose restrictions to $K_1\cap K_2$ are $\sigma|_{K_1\cap K_2}$
$\Rightarrow |H| = |\text{Gal}(K_1/F)| \cdot |\text{Gal}(K_2/K_1\cap K_2)|$
$= |\text{Gal}(K_1/F)| \cdot |\text{Gal}(K_2/F)| / |\text{Gal}(K_1\cap K_2/F)|$
By the last corollary, the orders of H, $\text{Gal}(K_1K_2/F)$ are
equal, and hence the gps are equal. ☐

Cor: If K_1, K_2 are Galois/F, with $K_1\cap K_2 = F$, then
$\text{Gal}(K_1K_2/F) \cong \text{Gal}(K_1/F) \times \text{Gal}(K_2/F)$.
Conversely, if K/F is Galois and $G = \text{Gal}(K/F) = G_1 \times G_2$,
$G_1, G_2 \leq G$, then $K = K_1K_2$ for two Galois exts
K_1, K_2 of F and $K_1\cap K_2 = F$. (5)

take α-free pt. to get. sep.

Pf: The first statement is clear. Assume the notation of the second, and let $K_1 := K_{G_1}$, $K_2 := K_{G_2}$. (consider the fixed fields)
Then $K_{G_1G_2} = K_1 \cap K_2$, and $G_1G_2 = G$, so $K_1 \cap K_2 = F$.
Moreover, $K_1K_2 = K'_{G_1 \cap K_2} = K_1 = K$. ☐

Important corollary:

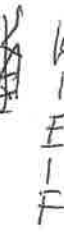
If E/F is finite separable, then E is contained in an ext^n K Galois over F such that, in a fixed alg. closure $\bar{K}$, any other Galois ext^n of F containing E contains K.
This is called the Galois closure of E/F.

Pf: It is easy to construct a Galois extension of F containing E, say the composite of all the splitting fields of all the minimal polys for a basis of E over F. Then these are all separable as E/F is. The intersection of all the Galois extensions of F containing E is our desired Galois closure

...mitive elements:

Thm: K/F is simple $\Leftrightarrow \exists$ finitely many intermediate fields

Def: $K = F(\theta) \rightarrow \theta$ is a primitive elt.



Pf: If K is simple, say $K = F(\theta)$, then let $f(x)$ be the min poly of θ over F, and for any intermediate field, let $g(x)$ be the min poly of θ over E. Now $f(x), g(x) \in E[x]$, and $g(x) \mid f(x)$.

If E' is F adjoin the coefficients of $g(x)$, then $E' \subseteq E$ and $\text{min poly}_{E'}(\theta) = g(x)$

$\Rightarrow [K : E'] = \deg(g(x)) = [K : E] \Rightarrow E = E'$

$\Rightarrow$ all intermediate fields are generated by the coeffs. of monic factors of $f(x) \Rightarrow \exists$ finitely many.

Conversely, suppose there are only finitely many intermediate fields. $|F| < \infty \Rightarrow K/F$ is an extension of finite fields, and as above ~~[illegible]~~ as $F_{p^n}^*$ is cyclic specifically, we have that K/F is simple.

Thus, we can assume $|F| = \infty$, and since K/F is finitely generated, it's enough to show that adjoining two elts can always be attained by adjoining only one; that is, $\forall \alpha, \beta \in K$, that $F(\alpha, \beta) = F(\gamma)$, some $\gamma \in K$.

Clearly, for any $c \in F$, $F \subseteq F(\alpha + c\beta) \subseteq F(\alpha, \beta)$. (7)

By assumption, there are infinitely many choices of c, and only finitely many intermediate fields, Hence there are distinct $c, c' \in F$.

$$F(\alpha + c\beta) = F(\alpha + c'\beta)$$

$\Rightarrow \alpha + c\beta, \alpha + c'\beta \in F(\alpha + c\beta) \Rightarrow (c - c')\beta \in F(\alpha + c\beta)$ (difference)

$\Rightarrow \beta \in F(\alpha + c\beta)$. By combining with $\alpha + c\beta \in F(\alpha + c\beta)$

$\alpha \in F(\alpha + c\beta) \Rightarrow F(\alpha, \beta) \subseteq F(\alpha + c\beta)$

$\Rightarrow F(\alpha, \beta) = F(\alpha + c\beta) \Rightarrow \alpha + c\beta$ is a primitive el't. ☐

Cor (Primitive El't. Theorem)

K/F finite + separable $\Rightarrow K/F$ simple.

Pf: If L is the Galois closure, then intermediate fields of b/w F and K are fixed fields of $Gal(L/F)$. But there are only finitely many of these subgps (a subgp. of) $\Rightarrow$ (Thm) K/F simple.

Cor: Finite exts of perfect fields are simple.

Ex: Using proof of primitive elt. theorem constructively:

$K = \mathbb{Q}(i, \sqrt[3]{2})/\mathbb{Q}$. Want to find α values where $c, c' \in \mathbb{Q}$, $\mathbb{Q}(i + c\sqrt[3]{2}) = \mathbb{Q}(i + c'\sqrt[3]{2})$

Another good general idea! $f(x) := x^2+1$ (min poly. of i)
$g(x) = x^3 - 2$ (min poly $\sqrt[3]{2}$)

Want: Find a primitive elt. $\alpha = i + c\sqrt[3]{2}$ which contains $\sqrt[3]{2}$ and also $i = \alpha - c\sqrt[3]{2}$. Want min poly of $\sqrt[3]{2}$ over $\mathbb{Q}(\alpha)$ is of degree 1. Note! $\sqrt[3]{2}$ satisfies $f(\alpha - c\sqrt[3]{2}) = f(i) = 0$

$\Rightarrow \sqrt[3]{2}$ a root of $h(x) := f(\alpha - cx) \Rightarrow$ min poly of $\sqrt[3]{2}$ over $\mathbb{Q}(\alpha)$ divides $g(x)$ and $h(x)$.

Want: gcd of g, h in $\mathbb{Q}(\alpha)[x]$ has deg < 2. Suppose $\deg(g,h) \geq 2$. Then g, h have a common root $\beta \neq \sqrt[3]{2} \in \mathrm{Split}(f, g)$ (x^3-2 separable $\Rightarrow$ $=L$)

$\Rightarrow f(\alpha - c\beta) = 0$, i.e., $\alpha - c\beta = a$, or a root of f in L.

As $\alpha = a + ci + c\sqrt[3]{2}$, we get $\alpha' + c\sqrt[3]{2} - c\beta = a$, or

$c = \frac{a - i}{\sqrt[3]{2} - \beta}$. Thus a bad choice of c [illegible] one that's of the form $c = \frac{\alpha' - \alpha}{\beta' - \beta}$

$c = \frac{\alpha - i}{\sqrt[3]{2} - \beta}$, α a root of x^2+1, $\beta \neq \sqrt[3]{2}$ a root of $x^3 - 2$.

(10) There are only finitely many bad ones