Lecture Notes from Math 412, Fall 2018

Kyle Ormsby

November 13, 2018

Contents

Galois
- Born 1811
- Published at age 18
- Cursed out examiner at École Polytechnique (denied entry)
- Expelled from École Normale for political editorial
- Joined a Republican artillery unit of the National Guard that was then disbanded for plotting a coup.
- Imprisoned for six months after political protest
- Killed in a duel. Final words to his younger brother: "Don't cry, Alfred! I need all my courage to die at twenty!"
- Mathematical testament written night before death outlined his work. "Ask Jacobi or Gauss to publicly give their opinion, not as to the truth, but as to the importance of these theorems. Later, there will be, I hope, some people who will find it to their advantage to decipher all this mess." Indeed — us!

Main idea Translate properties of algebraic solutions to polynomial equations into properties of the Galois group of automorphisms of the splitting field.

2.1 Polynomials of several variables

Variables $x_1, x_2, \ldots, x_n$

For F a field, $F[x_1, \ldots, x_n] = \{$polynomials in $x_1, \ldots, x_n$ with coefficients in $F\}$

Monomial: $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, $a_i \in \mathbb{N}$

Term: $c\, x_1^{a_1} \cdots x_n^{a_n}$, $c \in F$

Polynomial: sum of terms

The <u>degree</u> of a term $cx_1^{a_1}\cdots x_n^{a_n}$ is $a_1+\cdots+a_n$ $(c\neq 0)$.
The <u>degree</u> $\deg(f)$ of a polynomial f is the maximal degree of its terms $(f\neq 0)$. Define $\deg(0) = -\infty$.

<u>Check</u> $\deg(fg) = \deg(f)+\deg(g)$.

<u>Think Pair Share</u> Why does this imply that $F[x_1,\dots,x_n]$ is an integral domain? (No zero divisors.)

<u>Thm</u> $F[x_1,\dots,x_n]$ is a unique factorization domain.

<u>Rmk</u> But for $n>1$, $F[x_1,\dots,x_n]$ is not a PID!

<u>Thm</u> F a field, R an F-algebra (commutative ring containing F). Then for any set function $f:\{x_1,\dots,x_n\}\longrightarrow R$ there is a unique ring homomorphism $g: F[x_1,\dots,x_n]\longrightarrow R$ such that $g(x_i) = f(x_i)$, $i=1,\dots,n$. I.e.

$$\begin{tikzcd} x_i \arrow[d, mapsto] & \{x_1,\dots,x_n\} \arrow[r, "f"] \arrow[d] & R \\ x_i & F[x_1,\dots,x_n] \arrow[ur, dashed, "\exists! g"'] & \end{tikzcd}$$

<u>Rmk</u> · g is <u>evaluation</u> at $f(x_1),\dots,f(x_n)$:

$$g: h(x_1,\dots,x_n)\longmapsto h(f(x_1),\dots,f(x_n))$$

· Say that $F[x_1,\dots,x_n]$ is the <u>free F-algebra</u> on $\{x_1,\dots,x_n\}$.

<u>Dfn</u> $x_1,\dots,x_n$ variables over a field F. The <u>elementary symmetric polynomials</u> $\sigma_1,\dots,\sigma_n\in F[x_1,\dots,x_n]$ are

$$\sigma_1 := x_1+\cdots+x_n$$

$$\sigma_2 := \sum_{1\le i<j\le n} x_ix_j$$

$$\sigma_3 := \sum_{1\le i<j<k\le n} x_ix_jx_k$$

$$\vdots$$

$$\sigma_r := \sum_{1\le i_1<i_2<\cdots<i_r\le n} x_{i_1}x_{i_2}\cdots x_{i_r}$$

$$\vdots$$

$$\sigma_n := x_1x_2\cdots x_n$$

<u>Prop</u> $(x-x_1)(x-x_2)\cdots(x-x_n) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \cdots + (-1)^n \sigma_n$

i.e. $\prod_{i=1}^{n}(x-x_i) = \sum_{i=0}^{n}(-1)^i \sigma_i x^{n-i}$ where $\sigma_0 := 1$.

<u>Pf</u> When multiplying out $\prod_{i=1}^{n}(x-x_i)$, we get an x^{n-i} term when we take $n-i$ x's and i x_j's, each of which comes with a (-1) coefficient. Thus the coefficient of x^{n-i} is

$$\sum_{1\le j_1<j_2<\cdots<j_i\le n} (-1)^i x_{j_1} x_{j_2}\cdots x_{j_i} = (-1)^i \sigma_i . \qquad \square$$

<u>Cor</u> If $f = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in F[x]$ has roots $\alpha_1, \dots, \alpha_n \in L \supseteq F$, then $a_r = (-1)^r \sigma_r(\alpha_1, \dots, \alpha_n)$. $\square$

Symmetric Polynomials

$G \circlearrowright S$ — group G, (left) G-set S

$S^G := \{s \in S \mid g \cdot s = s\}$ is the G-fixed set of S. (or G-invariants)

$\Sigma_n = S_n$ = permutations of $\{1, 2, \dots, n\}$ = symmetric group on n letters

$\Sigma_n \circlearrowright F[x_1, \dots, x_n]$ by permuting variables:

$$\sigma \cdot f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

Moral Exercise: Check that this is an action: $e \cdot f = f$, $(\sigma\tau)f = \sigma(\tau f)$.

TPS: $\sigma \cdot (f+g) = \sigma f + \sigma g$, $\sigma \cdot (fg) = (\sigma f)(\sigma g)$ and thus $F[x_1, \dots, x_n]^{\Sigma_n}$ is a ring.

Thm: $F[x_1, \dots, x_n]^{\Sigma_n} = F[\sigma_1, \dots, \sigma_n]$, i.e., every symmetric polynomial is a polynomial in elementary symmetric polynomials. (and this expression is unique).

e.g. $x^3 + y^3 = (x+y)^3 - 3xy(x+y) = \sigma_1^3 - 3\sigma_1\sigma_2$.

Our proof uses graded lexicographic monomial order:

$$x_1^{a_1} \cdots x_n^{a_n} < x_1^{b_1} \cdots x_n^{b_n} \iff a_1 + \cdots + a_n < b_1 + \cdots + b_n$$

or $\Sigma a_i = \Sigma b_i$ & $a_1 < b_1$

or $\Sigma a_i = \Sigma b_i$, $a_1 = b_1$, & $a_2 < b_2$

or $\Sigma a_i = \Sigma b_i$, $a_1 = b_1$, $a_2 = b_2$, & $a_3 < b_3$

or ...

e.g. $x_1^4 x_2^2 x_3 < x_1^2 x_2^3 x_3^3$, $x_1^4 x_2^2 x_3 > x_1^4 x_2 x_3^2$.

TPS: Fix a monomial $x_1^{a_1} \cdots x_n^{a_n}$. Show that $\{x_1^{b_1} \cdots x_n^{b_n} < x_1^{a_1} \cdots x_n^{a_n}\}$ is finite.

Defn: The (graded lexicographic) leading term of $f \neq 0 \in F[x_1, \dots, x_n]$ is the term of f with largest monomial in the grlex order.

Pf of Thm: Take $f \underset{\neq 0}{\in} F[x_1, \dots, x_n]^{\Sigma_n}$ with leading term $c x_1^{a_1} \cdots x_n^{a_n}$. By symmetry, $a_1 \geq a_2 \geq \cdots \geq a_n$ (check this!).

Set $g = \sigma_1^{a_1-a_2}\sigma_2^{a_2-a_3}\cdots\sigma_{n-1}^{a_{n-1}-a_n}\sigma_n^{a_n}$ and check that the leading term of g is $x_1^{a_1}\cdots x_n^{a_n}$. Hence $f_1 = f - cg$ has a strictly smaller leading term and is also symmetric.

Repeat this process to produce $f_2 = f_1 - c_1 g_1 = f - cg - c_1 g_1$, $f_3 = f - cg - c_1g_1 - c_2g_2$, etc. with $c_i \in F^\times$, g_i polynomials in $\sigma_1, \dots, \sigma_n$. At each stage, the leading term gets strictly smaller.

TPS Why does this process terminate with some $f_m = 0$?

If $f_m = f - cg - c_1 g_1 - \cdots - c_{m-1}g_{m-1} = 0$, then

$$f = cg + c_1 g_1 + \cdots + c_{m-1}g_{m-1}.$$

Uniqueness: Read the proof of Thm 2.2.7 in the textbook. $\square$

Note Uniqueness tells us $\sigma_1, \dots, \sigma_n$ are algebraically independent.

Write $\Sigma_n x_1^{a_1}\cdots x_n^{a_n} := \sum \Sigma_n\cdot\{x_1^{a_1}\cdots x_n^{a_n}\}$ so that

$\Sigma_2 x_1^2x_2 = x_1^2x_2 + x_2^2x_1$ add together everything in the Σ_n-orbit.

$\Sigma_3 x_1^2x_2 = x_1^2x_2 + x_2^2x_1 + x_1^2x_3 + x_3^2x_1 + x_2^2x_3 + x_3^2x_2.$

The discriminant

For $n \geq 2$ variables $x_1, \dots, x_n$ over a field F, the <u>discriminant</u> is

$$\Delta := \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \in F[x_1, \dots, x_n].$$

$$= \left(\prod_{\substack{i \neq j \\ 1 \leq i,j \leq n}} (x_i - x_j) \right) \cdot (-1)^{\binom{n}{2}} \in F[x_1, \dots, x_n]^{\Sigma_n}.$$

Taking square root:

$$\sqrt{\Delta} = \prod_{1 \leq i < j \leq n} (x_i - x_j) \in F[x_1, \dots, x_n]$$

<u>Prop</u> For $\sigma \in \Sigma_n$, $\sigma \cdot \sqrt{\Delta} = \operatorname{sgn}(\sigma) \sqrt{\Delta}$

<u>Pf</u> HW! $\square$

Now define the discriminant of a polynomial $f = x^n + a_1 x^{n-1} + \dots + a_n \in F[x]$.

Let $\tilde{f} = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \dots + (-1)^n \sigma_n \in F[x, x_1, \dots, x_n]$.

Then $\tilde{f} \mapsto f$ under the map taking σ_i to $(-1)^i a_i$ (evaluation on $F[x, \sigma_1, \dots, \sigma_n]$).

<u>Defn</u> $\Delta(f) = \Delta(-a_1, a_2, \dots, (-1)^n a_n)$ where $\Delta = \Delta(\sigma_1, \dots, \sigma_n)$.

$\Delta(f) := 1$ if f has degree 1.

<u>e.g.</u> $f = x^2 + bx + c$

$\Delta = x_1^2 - 2x_1x_2 + x_2^2 = \sigma_1^2 - 4\sigma_2$

$\Rightarrow \Delta(f) = b^2 - 4c$.

<u>Prop</u> If $f \in F[x]$ monic of deg $n \geq 2$ has roots $\alpha_1, \dots, \alpha_n$ in $L \supseteq F$, then $\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$.

<u>Pf</u> Consider the evaluation map $x_i \mapsto \alpha_i$; then $\Delta \mapsto \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$.

If $\Delta = \Delta(\sigma_1, \dots, \sigma_n)$, then $x_i \mapsto \alpha_i$ takes Δ to

$\Delta(\sigma_1(\alpha_1, \dots, \alpha_n), \dots, \sigma_n(\alpha_1, \dots, \alpha_n)) = \Delta(-a_1, a_2, \dots, (-1)^n a_n) = \Delta(f)$. $\square$

Note Let $R = F[x_1, \dots, x_n]$ and $A_n = \ker(\mathrm{sgn}) \leq \Sigma_n$ denote the alternating group. Then $R^{\Sigma_n} \subseteq R^{A_n} \subseteq R$ and $\sqrt{\Delta}$ is an example of an element of $R^{A_n} \setminus R^{\Sigma_n}$. In fact,

$$R^{A_n} = R^{\Sigma_n}[\sqrt{\Delta}] \Big/ ((\sqrt{\Delta})^2 - \Delta) = F[\sigma_1, \dots, \sigma_n, \sqrt{\Delta}] \Big/ (\sqrt{\Delta}^2 - \Delta) .$$

We'll prove a function field version of this in Ch. 7.

Prop
$$\sqrt{\Delta} = \det \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix} \cdot (-1)^{n(n-1)/2}$$

Pf Call the matrix in question V. By the Leibniz (permutation) expansion of $\det V$,

$$\det V = \sum_{\sigma \in \Sigma_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} x_{\sigma(i)}^{i-1} .$$

Thus each term has degree $0 + 1 + \cdots + (n-1) = \frac{n(n-1)}{2}$.
If we set x_j equal to x_i $(i \neq j)$, V has two identical rows and thus 0 determinant. Thus $x_j - x_i$ is a factor of $\det V$.
Hence $\det V = g \cdot \sqrt{\Delta}$ for some polynomial g. Clearly ~~det~~ $\sqrt{\Delta}$ is homogeneous of degree $\frac{n(n-1)}{2}$ so g is constant.
The $\sigma = e$ contribution to $\det V$ is $x_2 x_3^2 \cdots x_n^{n-1}$ which equals the summand of $\sqrt{\Delta}$ given by multiplying all first terms in $(x_2 - x_1)(x_3 - x_1)(x_3 - x_2)(x_4 - x_1)(x_4 - x_2)(x_4 - x_3) \cdots$.
Hence $g = 1$ and $\sqrt{\Delta} = \det V$. $\square$

As written, proof neglects the sign — spot the mistake!

Existence of Roots

Two perspectives on $\mathbb{C}$:

Hamilton: $\mathbb{C} = \mathbb{R}^2$ with $(a,b)\cdot(c,d) = (ac-bd, ad+bc)$

Cauchy: $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$. Mult'n law derives from taking remainder of $(a+bx)(c+dx)$ upon division by x^2+1. Field b/c $(x^2+1) \subseteq \mathbb{R}[x]$ is a maximal ideal:

Prop If F is a field and $f \in F[x]$ is nonconstant, then TFAE

(a) The poly f is irreducible over F.

(b) The ideal $(f) = \{fg \mid g \in F[x]\}$ is maximal.

(c) The quotient ring $F[x]/(f)$ is a field.

Pf (b) $\Leftrightarrow$ (c) is standard.

(a) $\Rightarrow$ (b). Suppose f irred, $(f) \subseteq \overset{\text{ideal}}{I} \subseteq F[x]$. Since $F[x]$ is a PID, $I = (g)$ for some $g \in F[x]$. Then $f \in (g)$ implies $f = gh$ for some $h \in F[x]$. Since f is irred, g or h must be constant. If g constant, $I = F[x]$. If h constant, $I = (f)$.

(b) $\Rightarrow$ (a). Suppose (f) max'l and let $f = gh$. Then $(f) \subseteq (g)$ so $(g) = (f)$ or $F[x]$. The former implies h constant, the latter g constant. Thus f irred. $\square$

Since x^2+1 irred$/\mathbb{R}$ (TPS: Why?) we deduce (x^2+1) max'l so $\mathbb{R}[x]/(x^2+1)$ is a field.

Defn Given a ring homomorphism of fields $\varphi: F \to L$, say L is a field extension of F via φ. Usually identify F with its image $\varphi(F) \subseteq L$, and write $F \subseteq L$.

HW φ is injective inducing $F \cong \varphi(F)$.

Notation Write L/F when L is a field extension of F.

Prop If $f \in F[x]$ is irreducible, then there exists L/F and $\alpha \in L$ s.t. $f(\alpha) = 0$.

Pf Let $L = F[x]/(f) \xleftarrow{\varphi} F$. Set $\alpha = x + (f)$.

$a + (f) \longleftarrow a$

Suppose $f = a_0 x^n + \cdots + a_n$ w/ $a_i \in F$. Then

$$f(\alpha) = (a_0 + (f))(x + (f))^n + \cdots + (a_n + (f))$$
$$= a_0 x^n + \cdots + a_n + (f)$$
$$= f + (f) = 0 + (f). \quad \square$$

Recall $\alpha \in L$ is a root of $f \in L[x]$ iff $x - \alpha$ is a factor of f in $L[x]$.

A field L contains all roots of f means f factors

$$f = a_0 (x - \alpha_1) \cdots (x - \alpha_n)$$

where $\alpha_1, \dots, \alpha_n \in L$. When this happens, we say f *splits completely* over L.

Thm Let $f \in F[x]$ be a poly of degree $n > 0$. Then $\exists\, L/F$ s.t. f splits completely over L.

Pf by induction on $n = \deg(f)$. If $n = 1$, $f = a_0 x + a_1$, $a_0 \neq 0$, $a_0, a_1 \in F$. Then $L = F$, $\alpha_1 = -a_1/a_0 \Rightarrow f = a_0(x - \alpha_1)$.

Now suppose $\deg(f) = n > 1$ & thm is true for $n-1$. Since $F[x]$ is a UFD, f has an irred divisor f_1. $\exists\, F_1/F$ and $\alpha_1 \in F_1$ s.t. $f_1(\alpha_1) = 0 \Rightarrow f(\alpha_1) = 0$ in F_1. Thus $f = (x - \alpha_1) g$ for some $g \in F_1[x]$ of deg $n-1$. Applying the induction hypothesis to g gives L/F_1 and $\alpha_2, \dots, \alpha_n \in L$ s.t. $g = a_0(x - \alpha_2) \cdots (x - \alpha_n)$. Thus $f = a_0(x - \alpha_1) \cdots (x - \alpha_n)$ so f splits completely over L. $\square$

Fundamental Theorem of Algebra Every nonconstant $f \in \mathbb{C}[x]$ splits completely over $\mathbb{C}$, i.e. $f = a_0(x-\alpha_1)\cdots(x-\alpha_n)$ for some $a_0, \alpha_1, \ldots, \alpha_n \in \mathbb{C}$ with $a_0 \neq 0$.

Prop TFAE:

(a) Every nonconst $f \in \mathbb{C}[x]$ has at least one root in $\mathbb{C}$.

(b) Every nonconst $f \in \mathbb{C}[x]$ splits completely over $\mathbb{C}$.

(c) Every nonconst $f \in \mathbb{R}[x]$ has at least one root in $\mathbb{C}$.

Sketch (a) $\Rightarrow$ (b) by induction on degree.

(b) $\Rightarrow$ (c) is trivial since $\mathbb{R} \subseteq \mathbb{C}$.

For (c) $\Rightarrow$ (a), take $f = a_0x^n + \cdots + a_n \in \mathbb{C}[x]$. We must show that f has a root in $\mathbb{C}$ when $n>0$, $a_0 \neq 0$. Define $\bar{f} = \bar{a}_0x^n + \cdots + \bar{a}_n$. Check $\bar{f}\bar{g} = \overline{fg}$. Hence $\overline{f\bar{f}} = \bar{f}\bar{\bar{f}} = \bar{f}f = f\bar{f} \Rightarrow f\bar{f} \in \mathbb{R}[x]$.

By hypothesis, $\exists \alpha \in \mathbb{C}$ s.t. $(f\bar{f})(\alpha) = 0$. But then $f(\alpha)\bar{f}(\alpha) = 0$ so $f(\alpha) = 0$ or $\bar{f}(\alpha) = 0$. In the former case, $\alpha \in \mathbb{C}$ is a root of f; in the latter, $\bar{\alpha} \in \mathbb{C}$ is a root of f (check!). $\square$

Prop Every $f \in \mathbb{R}[x]$ of odd degree has at least one root in $\mathbb{R}$.

Sketch WLOG, $f = x^n + a_1x^{n-1} + \cdots + a_n$ with n odd, $a_1, \ldots, a_n \in \mathbb{R}$. For $x \gg 0$, $f(x) > 0$. For $x \ll 0$, $f(x) < 0$. Thus, by the intermediate value theorem (Math 112!), f has a root. $\square$

Lemma Every quadratic polynomial in $\mathbb{C}[x]$ splits completely over $\mathbb{C}$.

Pf The roots of $f = ax^2 + bx + c$ with $a \neq 0$ are $\dfrac{-b \pm \sqrt{b^2-4ac}}{2a}$.

$b^2 - 4ac = re^{i\theta}$ for some $r \geq 0 \in \mathbb{R}$. Hence

$\sqrt{b^2-4ac} = \sqrt{r}\, e^{i\theta/2} \in \mathbb{C}$ since $\sqrt{r}$ exists (again by IVT).

Hence the roots of f are in $\mathbb{C}$.

$\square$

Pf of FTA It suffices to show that every $f \in \mathbb{R}[x]$ of deg $n > 0$ has at least one root in $\mathbb{C}$. Write n as $n = 2^m k$, k odd, $m \geq 0$. We proceed by induction on m. If $m = 0$, $\deg(f) = k$ odd, so we're done by the Prop.

Now suppose $m > 0$ and every $f \in \mathbb{R}[x]$ of degree $2^{m-1} \cdot (\text{odd})$ has at least one root in $\mathbb{C}$. $\exists\, L/\mathbb{C}$ s.t. f splits completely over L with roots $\alpha_1, \dots, \alpha_n \in L$.

Clever idea (Laplace): Set $g_\lambda(x) = \prod_{1 \leq i < j \leq n} (x - (\alpha_i + \alpha_j) + \lambda \alpha_i \alpha_j)$

where $\lambda \in \mathbb{R}$. $\deg(g_\lambda) = \frac{1}{2} n(n-1)$.

Claim $g_\lambda \in \mathbb{R}[x]$.

Justification Consider $G_\lambda(x) = \prod_{1 \leq i < j \leq n} (x - (x_i + x_j) + \lambda x_i x_j)$

G_λ is fixed by transpositions and hence by Σ_n. It follows that there are symmetric polynomials $p_i(x_1, \dots, x_n)$ s.t. $G_\lambda(x) = \sum_{i=0}^{\frac{1}{2}n(n-1)} p_i(x_1, \dots, x_n) x^i$. Since $\lambda \in \mathbb{R}$, $p_i \in \mathbb{R}[x_1, \dots, x_n]$.

By Cor 2.2.5, $p_i(\alpha_1, \dots, \alpha_n) \in \mathbb{R}$ since $\alpha_1, \dots, \alpha_n$ are the roots of $f \in \mathbb{R}[x]$. Thus $g_\lambda(x) = \sum_{i=0}^{\frac{1}{2}n(n-1)} p_i(\alpha_1, \dots, \alpha_n) x^i \in \mathbb{R}[x]$.

Now $\deg(g_\lambda) = \frac{1}{2} n(n-1) = \frac{1}{2} 2^m k (2^m k - 1) = 2^{m-1} \underbrace{k (2^m k - 1)}_{\text{odd}}$

Thus the induction hypothesis applies and g_λ has a root in $\mathbb{C}$. These roots are $\alpha_i + \alpha_j - \lambda \alpha_i \alpha_j$, so for each $\lambda \in \mathbb{R}$ we can find a pair i, j with $1 \leq i < j \leq n$ s.t. $\alpha_i + \alpha_j - \lambda \alpha_i \alpha_j \in \mathbb{C}$.

By the infinite $\to$ finite pigeonhole principle, $\exists\, \lambda \neq \mu \in \mathbb{R}$ and $1 \leq i < j \leq n$ s.t. $\alpha_i + \alpha_j - \lambda \alpha_i \alpha_j \in \mathbb{C}$ and $\alpha_i + \alpha_j - \mu \alpha_i \alpha_j \in \mathbb{C}$.

Subtracting, $(\mu-\lambda)\alpha_i\alpha_j \in \mathbb{C} \Rightarrow \alpha_i\alpha_j \in \mathbb{C} \Rightarrow \alpha_i+\alpha_j \in \mathbb{C}$.

Now consider the quadratic polynomial

$$(x-\alpha_i)(x-\alpha_j) = x^2-(\alpha_i+\alpha_j)+\alpha_i\alpha_j .$$

This has coeffs in $\mathbb{C}$ and hence roots in $\mathbb{C}$, so $\alpha_i, \alpha_j \in \mathbb{C}$. $\square$

Elements of Extension Fields

Defn Extension L/F, $\alpha \in L$. Then α is algebraic over F if there is a nonconstant polynomial $f \in F[x]$ s.t. $f(\alpha) = 0$. If α is not algebraic over F, then α is transcendental over F.

e.g.
- $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ since $\sqrt{2}$ is a root of $x^2 - 2 \in \mathbb{Q}[x]$
- $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ since it's a root of $x^n - 1 \in \mathbb{Q}[x]$.
- π, e are transcendental over $\mathbb{Q}$ [hard!]
- $\sqrt{2} + \sqrt{3}$ is a root of $(x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3})$ $= x^4 - 10x^2 + 1$ so is algebraic over $\mathbb{Q}$.
- Next Monday: If $\alpha, \beta \in L$ are alg over F, then so are $\alpha + \beta$, $\alpha\beta$, $\frac{1}{\alpha}$. Thus $\{\alpha \in L \mid \alpha \text{ alg}/F\}$ is a subfield of L.

Lemma If $\alpha \in L$ alg $/F$, then $\exists!$ nonconst monic poly $p \in F[x]$ s.t.

(a) $p(\alpha) = 0$, and

(b) if $f \in F[x]$ with $f(\alpha) = 0$, then $p \mid f$.

Defn Such p is called the minimal polynomial of α over F.

Pf of Lemma Among nonconstant $f \in F[x]$ w/ α as a root, there is (at least) one with minimal degree. Dividing by leading coeff, call this p. Clearly $p(\alpha) = 0$. Now suppose $f(\alpha) = 0$. Then $f = qp + r$ for some $q, r \in F[x]$ with $r = 0$ or $\deg(r) < \deg(p)$. Eval'n at α gives $0 = f(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = r(\alpha)$. By minimality of $\deg(p)$, we conclude $r = 0$.

Uniqueness: ~~So~~ suppose $\tilde{p}$ also satisfies (a), (b). We get $p \mid \tilde{p}$ & $\tilde{p} \mid p$. Since both are monic, $p = \tilde{p}$. $\square$

Prop $\alpha \in L$ alg $/F$, p = min poly of α $/F$. If $f \in F[x]$ is a nonconstant monic polynomial, then $f = p$ iff f is a poly of min'l degree with $f(\alpha) = 0$ iff f is irred $/F$ with $f(\alpha) = 0$.

Pf First equiv is in the proof of the lemma. Now show min poly is irred: if not, one of its factors has lower degree & α as root, contradicting first criterion. Now suppose $f(\alpha)=0$ with f irred. Then $p \mid f \Rightarrow p=f$ since both monic, f irred. $\square$

e.g. • $p_{\sqrt{2},\mathbb{Q}} = x^2-2$

• $p_{\sqrt{2}+\sqrt{3},\mathbb{Q}} = x^4-10x^2+1$

• $p_{\zeta_n,\mathbb{Q}} = \Phi_n$, n-th cyclotomic poly of degree $\phi(n) = \#$divisors of n. $(1\le k\le n)$

Adjoining elts Given $\alpha_1,\dots,\alpha_n \in L$, define $F[\alpha_1,\dots,\alpha_n] := \{h(\alpha_1,\dots,\alpha_n) \mid h\in F[x_1,\dots,x_n]\}$, $F(\alpha_1,\dots,\alpha_n) := \mathrm{Frac}(F[\alpha_1,\dots,\alpha_n])$

Lemma $F(\alpha_1,\dots,\alpha_n)$ is the smallest subfield of L containing F and $\alpha_1,\dots,\alpha_n$.

Pf Must show that if K/F, $\alpha_1,\dots,\alpha_n\in K$, then $F(\alpha_1,\dots,\alpha_n)\subseteq K$. Obvious since $F[\alpha_1,\dots,\alpha_n]\subseteq K$ & K is a field. $\square$

Cor $F(\alpha_1,\dots,\alpha_n) = F(\alpha_1,\dots,\alpha_r)(\alpha_{r+1},\dots,\alpha_n)$. $\square$

Lemma L/F, $\alpha\in L$ alg over F with min poly $p\in F[x]$. Then $\exists!$ ring iso $F[\alpha]\cong F[x]/(p)$ which is the identity on F w/ $\alpha\mapsto x+(p)$.

Pf Take $\varphi: F[x]\to L$, $x\mapsto\alpha$, which has image $F[\alpha]$. Remains to show $\ker(\varphi)=(p)$. Since $p(\alpha)=0$, $p\in\ker\varphi$ so $(p)\subseteq\ker\varphi$. If $f\in\ker\varphi$, $f(\alpha)=0$ so $p\mid f$ so $\ker\varphi\subseteq(p)$.

Uniqueness: ring hom defined on $F[\alpha]$ is determined by its values on F,α. $\square$

Prop L/F, $\alpha \in L$. Then α is algebraic over F iff $F[\alpha] = F(\alpha)$.

Pf Lemma + $F[x]/(p)$ a field for p irred gives $\Rightarrow$.

($\Leftarrow$) Assume $\alpha \neq 0$. Then $\frac{1}{\alpha} \in F(\alpha) = F[\alpha]$ implies

$$\frac{1}{\alpha} = a_0 + a_1\alpha + \cdots + a_m\alpha^m.$$

for some $a_i \in F$. Thus $0 = -1 + a_0\alpha + a_1\alpha^2 + \cdots + a_m\alpha^{m+1}$ so α alg$/F$. $\square$

Prop $F \subseteq L \ni \alpha_1, \dots, \alpha_n$ alg $/F$. Then $F[\alpha_1, \dots, \alpha_n] = F(\alpha_1, \dots, \alpha_n)$.

Pf by induction on n. $\square$

Irreducible Polynomials

Gauss's Lemma Suppose $f \in \mathbb{Z}[x]$ nonconstant and $f = gh$ where $g, h \in \mathbb{Q}[x]$. Then $\exists \delta \in \mathbb{Q}^\times$ s.t. $\tilde{g} = \delta g$, $\tilde{h} = \delta^{-1} h \in \mathbb{Z}[x]$ (and thus $f = \tilde{g}\tilde{h}$ in $\mathbb{Z}[x]$).

Pf p.529 □

Cor If $f \in \mathbb{Z}[x]$ has positive degree and is reducible over $\mathbb{Q}$, then $f = gh$ where $g, h \in \mathbb{Z}[x]$ have degrees $< \deg(f)$. □

Algorithm for irreducibility of $f \in \mathbb{Z}[x]$:

- WLOG, assume $f(0), f(1), \ldots, f(n-1) \neq 0$.
- Fix integer $0 < d \leq n$.
- Fix divisors $a_0, \ldots, a_d \in \mathbb{Z}$ of $f(0), \ldots, f(d) \in \mathbb{Z}$.
- Construct $g \in \mathbb{Q}[x]$ of degree $\leq d$ s.t. $g(i) = a_i$ for $i = 0, \ldots, d$ (Lagrange interpolation)
- Accept g if it has degree d and integer coeffs; reject it o/w.
- ~~Get~~ Do this for all $0 < d \leq n$, $a_0 | f(0), \ldots, a_d | f(d)$ to get a set of "accepted" $g \in \mathbb{Z}[x]$.

Prop This set is finite, and f is irred/$\mathbb{Q}$ iff it is not divisible by any of the polynomials in this set.

Pf Each $f(i)$ has fin many divisors, and g is uniquely determined by $a_0, \ldots, a_d$, so we get only finitely many g this way. Remains to show f reducible iff some accepted g divides f.

($\Leftarrow$) ✓.

($\Rightarrow$) By the corollary, $f = gh$ where $g, h \in \mathbb{Z}[x]$, g has degree d, $0 < d \leq n$. For $0 \leq i \leq d$, set $a_i = g(i) \mid f(i)$. Lagrange interpolation gives $\tilde{g} \in \mathbb{Q}[x]$ with $\deg(\tilde{g}) \leq d$, $\tilde{g}(i) = a_i$. Then $\deg(g - \tilde{g}) \leq d$ and $(g - \tilde{g})(i) = 0$ for $0 \leq i \leq d$ ($d+1$ roots) so $g - \tilde{g} = 0 \Rightarrow g = \tilde{g}$ is in our list. □

Thm [Eisenstein criterion] Let $f = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$, $a_n \neq 0$, $n > 0$.
If there is a prime p s.t. $p \nmid a_n$, $p \mid a_{n-1}, \dots, p \mid a_0$, and $p^2 \nmid a_0$, then f is irreducible over $\mathbb{Q}$.

Pf Suppose for $\lightning$ f is of the above form & reducible over $\mathbb{Q}$.
Then $f = gh$ for $g, h \in \mathbb{Z}[x]$ of degree $< n$. Write $\overline{(\;)} : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ for the mod p reduction map. Then $\bar{a}_n x^n = \bar{g}\bar{h}$
$\Rightarrow \bar{g} = \bar{a} x^r$, $\bar{h} = \bar{b} x^s$ for $\bar{a}\bar{b} = \bar{a}_n$, $r + s = n$.

TPS ~~Whe~~ Why does $p \nmid a_n$ imply $r > 0, s > 0$?

Then $\bar{g} = \bar{a} x^r$ for $r > 0 \Rightarrow p$ divides constant term of g, and similarly for $h \Rightarrow p^2 \mid a_0$ $\lightning$. $\square$

e.g. $x^n + px + p$, $n \geq 2$, p prime irred $/\mathbb{Q}$

Prop $\Phi_p := x^{p-1} + x^{p-2} + \dots + 1$, p prime is irred $/\mathbb{Q}$.

Pf $\Phi_p(x+1) = \dfrac{(x+1)^p - 1}{x}$ and $(x+1)^p = x^p + \binom{p}{1} x^{p-1} + \dots + \binom{p}{p-1} x + 1$

so $\Phi_p(x+1) = x^{p-1} + \binom{p}{1} x^{p-2} + \dots + \binom{p}{p-1}$. By prime divisibility properties of binomial coeffs, this satisfies the Eisenstein criterion, so $\Phi_p(x+1)$ is irred. Then reducibility of $\Phi_p(x)$ would contradict this. $\square$

Prop For p prime, $f = x^p - a \in F[x]$ is irred $/F$ iff f has no roots in F.

Pf ($\Leftarrow$) ✓.

($\Rightarrow$) Assume f reducible. Take L/F for which f splits completely
$f = (x - \alpha_1) \cdots (x - \alpha_p)$, $\alpha_i \in L$. WLOG, $\alpha_1 \neq 0$. Set $\zeta_i = \dfrac{\alpha_i}{\alpha_1}$, $1 \leq i \leq p$. Then $\alpha_i^p \Rightarrow \zeta_i^p = 1$, so $\alpha_i = \zeta_i \alpha_1$ with ζ_i a pth root of unity: $f = (x - \zeta_1\alpha_1)(x - \zeta_2\alpha_1) \cdots (x - \zeta_p \alpha_1)$.
Suppose $f = gh$, $g, h \in F[x]$ monic with degrees $r, s < p$.

By unique fact'n + relabeling, $g = (x-\zeta_1\alpha_1)\cdots(x-\zeta_r\alpha_r)$.

Since the constant term of g is in F, $\underbrace{\zeta_1\cdots\zeta_r}_{\zeta}\alpha_1^r \in F$. Note $\zeta^p = 1$.

Since $0<r<p$, p prime, $\exists\, m,n \in \mathbb{Z}$ s.t. $mr+np=1$. Then

$\zeta^m\alpha_1 = \zeta^m\alpha_1^{mr+np} = (\underbrace{\zeta\alpha_1^r}_{\in F})^m(\underbrace{\alpha_1^p}_{a\in F})^n \in F$. Thus $(\zeta^m\alpha_1)^p = (\zeta^p)^m\alpha_1^p$

$= a \implies \zeta^m\alpha_1$ is a root of $f = x^p - a$ lying in F. $\square$

Degree

For any field extn L/F, L is an F-vector space.

Defn The degree of L/F is $[L:F] := \dim_F L$.

Call L/F a finite extension if $[L:F] < \infty$.

e.g.
- $[\mathbb{C}:\mathbb{R}] = 2$
- $[\mathbb{Q}(\sqrt{D}):\mathbb{Q}] = 2$ for D not a square in $\mathbb{Q}$.
- $[L:F] = 1$ iff $L = F$.

Prop $\alpha \in L/F$.

(a) α is alg $/F$ iff $[F(\alpha):F] < \infty$.

(b) Let α be alg $/F$. If n = degree of min poly of α/F, then $1, \alpha, \dots, \alpha^{n-1}$ form a basis of $F(\alpha)$ over F. Thus $[F(\alpha):F] = n$.

Pf First suppose α alg $/F$ w/ min poly p, $n = \deg(p)$. Since $F(\alpha) = F[\alpha]$, every elt of $F(\alpha)$ is of the form $g(\alpha)$ for some $g \in F[x]$.

By the division algorithm, $g = qp + (a_0 + a_1 x + \dots + a_{n-1} x^{n-1})$ w/ $q \in F[x]$, $a_i \in F$. Eval'n at $x = \alpha$ gives

$$g(\alpha) = a_0 + \dots + a_{n-1}\alpha^{n-1}$$

Hence $1, \dots, \alpha^{n-1}$ span $F(\alpha)$ over F. Linear independence follows from minimality of $\deg(p)$. Thus $[F(\alpha):F] = n < \infty$.

Now suppose $[F(\alpha):F] = n < \infty$. Then $1, \alpha, \dots, \alpha^n$ are lin dep over F. Hence $\exists a_i \in F$ s.t. $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$. $\square$

e.g. Since min poly of $\sqrt{2}+\sqrt{3}$ $/\mathbb{Q}$ is $x^4 - 10x^2 + 1$, $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = 4$ and every elt of $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ can be written uniquely in the form $a + b(\sqrt{2}+\sqrt{3}) + c(\sqrt{2}+\sqrt{3})^2 + d(\sqrt{2}+\sqrt{3})^3$, $a, b, c, d \in \mathbb{Q}$.

Towers

Thm Suppose we have fields $F \subseteq K \subseteq L$.

(a) If $[K:F] = \infty$ or $[L:K] = \infty$, then $[L:F] = \infty$.

(b) If $[K:F] < \infty$ and $[L:K] < \infty$, then $[L:F] = [L:K][K:F]$.

Diagrammatically:

$$\begin{tikzcd}
L \arrow[dd, dash, "mn"'] \arrow[dr, dash, "n"] & \\
& K \arrow[dl, dash, "m"] \\
F &
\end{tikzcd}$$

Pf (a) Suppose $[L:F] = N$ and let $\gamma_1, \dots, \gamma_N$ be a basis of L/F. Then K is an F-subspace of L, hence is finite dim'l $/F$, i.e. $[K:F] < \infty$. Take $\alpha \in L$. Then $\alpha = \sum_{i=1}^{N} a_i \gamma_i$ with $a_i \in F \subseteq K$, so L is spanned by $\gamma_1, \dots, \gamma_N$ as K-vs. $\Rightarrow [L:K] \leq n < \infty$.

(b) Let $m = [K:F]$, $n = [L:K]$, and pick bases $\alpha_1, \dots, \alpha_m$ of K/F, $\beta_1, \dots, \beta_n$ of L/K. Show $\{\alpha_i \beta_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ are a basis of L/F: For $\gamma \in L$, $\gamma = \sum_{j=1}^{n} b_j \beta_j$, $b_j \in K$, $b_j = \sum_{i=1}^{m} a_{ij} \alpha_i$, $a_{ij} \in F$.

Thus $\gamma = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} \alpha_i \beta_j$ so $\{\alpha_i \beta_j\}$ span L/F.

TBS Linear independence? $\square$

e.g. $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

Basis $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ of $\mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}$.

Note If we believe $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$, then

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dd, dash, "4"'] \arrow[dr, dash] & \\
& \mathbb{Q}(\sqrt{2} + \sqrt{3}) \arrow[dl, dash, "4"] \\
\mathbb{Q} &
\end{tikzcd} \Rightarrow \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

e.g. Let $\omega = e^{2\pi i/3}$.

$$\begin{tikzcd}
\mathbb{Q}(\omega, \sqrt[3]{2}) \arrow[dd, dash, "6"'] \arrow[dr, dash, "2"] & \\
& \mathbb{Q}(\sqrt[3]{2}) \arrow[dl, dash, "3"] \\
\mathbb{Q} &
\end{tikzcd}$$

2 b/c ω, ω^2 roots of $x^2 + x + 1$, $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ so $x^2 + x + 1 = $ min poly of $\omega / \mathbb{Q}(\sqrt[3]{2})$

3 b/c $x^3 - 2$ irred by Eisenstein

Algebraic Extensions

Defn A field extn L/F is algebraic if every element of L is algebraic over F.

Lemma Suppose L/F is finite. Then

(a) L/F is algebraic.

(b) If $\alpha \in L$, then $\deg(m_{\alpha,F}) \mid [L:F]$.

Pf For $\alpha \in L$, $F \subseteq F(\alpha) \subseteq L$ and the tower thm gives $[F(\alpha):F]$ finite, dividing $[L:F]$. We have already seen $[F(\alpha):F]$ finite $\Leftrightarrow$ α alg $/F$. $\square$

Note There are alg extns which are not finite.

Thm Let L/F be a field extn. Then $[L:F] < \infty$ iff $\exists \alpha_1, \dots, \alpha_m \in L$ s.t. each α_i is alg $/F$, and $L = F(\alpha_1, \dots, \alpha_m)$

Pf Suppose $[L:F] < \infty$ and take $\alpha_1, \dots, \alpha_m \in L$ a basis of L over F. Then $L = \{a_1\alpha_1 + \dots + a_m\alpha_m \mid a_i \in F\} \subseteq F(\alpha_1, \dots, \alpha_m) \subseteq L$ so $L = F(\alpha_1, \dots, \alpha_m)$ and Lemma shows each α_i alg $/F$.

Now suppose $L = F(\alpha_1, \dots, \alpha_m)$ with each α_i alg $/F$.

Let $L_0 = F$, $L_i = F(\alpha_1, \dots, \alpha_i)$ for $1 \le i \le m$. Get $F = L_0 \subseteq L_1 \subseteq \dots \subseteq L_m = L$. and $L_i = L_{i-1}(\alpha_i)$. Since α_i alg $/F$, it is also alg $/L_{i-1}$, so $[L_i : L_{i-1}] < \infty$. Thus $[L:F] = [L_m : L_{m-1}] \cdots [L_1 : L_0] < \infty$. $\square$

Prop Let L/F be a field extn. If $\alpha, \beta \in L$ alg $/F$, then $\alpha+\beta$, $\alpha\beta$ are alg $/F$ as well.

Pf By the thm, $F(\alpha,\beta)/F$ is a finite extn, hence algebraic. $\square$

Cor For any L/F, $M = \{\alpha \in L \mid \alpha \text{ alg}/F\}$ is a subfield of L containing F. $\square$

<u>Thm</u> Let $F \subseteq K \subseteq L$. If $\alpha \in L$ alg/K and K alg/F, then α alg/F.

<u>Pf</u> Let α be a root of $f = \beta_n x^n + \cdots + \beta_0 \in K[x]$ where $\beta_n, \ldots, \beta_0 \in K$, not all 0. Each β_i alg/F, so $M = F(\beta_n, \ldots, \beta_0)$ is a finite extn of F. Note $f \in M[x]$, so α alg/M, so $M(\alpha)/M$ is finite. Then $[M(\alpha):F] = [M(\alpha):M][M:F] < \infty$, so α alg/F. $\square$

<u>e.g.</u> Every cpx soln of $x^{11} - (\sqrt{2}+\sqrt{5})x^5 + 3\sqrt[4]{12}\,x^3 + (1+3i)x + \sqrt[5]{17} = 0$ is an algebraic number.

<u>Cor</u> $L/K/F$ with L/K alg, K/F alg, then L/F algebraic.

<u>Defn</u> The algebraic #s $\overline{\mathbb{Q}} = \{z \in \mathbb{C} \mid z \text{ alg}/\mathbb{Q}\}$.

<u>Thm</u> The field $\overline{\mathbb{Q}}$ is algebraically closed.

<u>Pf</u> It suffices to show every nonconstant poly in $\overline{\mathbb{Q}}[x]$ has a root in $\overline{\mathbb{Q}}$. Given such f, it has a root $\alpha \in \mathbb{C}$. Thus α alg/$\overline{\mathbb{Q}}$ since it's a root of $f \in \overline{\mathbb{Q}}[x]$. By the corollary, α alg/$\mathbb{Q}$ so $\alpha \in \overline{\mathbb{Q}}$. $\square$

Splitting Fields

Defn Let $f \in F[x]$ have degree $n > 0$. Then an extn L/F is a splitting field of f over F if
(a) $f = c(x-\alpha_1)\cdots(x-\alpha_n)$, $c \in F$, $\alpha_i \in L$, and
(b) $L = F(\alpha_1, \ldots, \alpha_n)$.

Note Such L is the smallest field over which f splits completely.

e.g. Splitting field of x^2+1 $/\mathbb{Q}$ is $\mathbb{Q}(i)$
$/\mathbb{R}$ is $\mathbb{C}$
$/\mathbb{C}$ is $\mathbb{C}$

e.g. Splitting field of x^4-2 $/\mathbb{Q}$ is $\mathbb{Q}(i, \sqrt[4]{2})$.

Thm Let $f \in F[x]$ have degree $n > 0$, and let L be a splitting field of f. Then $[L:F] \leq n!$.

Pf Proceed by induction on n. If $n=1$, $f = ax+b$ has root $-b/a \in F$, so $L = F$ and $[L:F] = 1 \leq 1!$.
Now suppose f has degree $n > 1$, $L = F(\alpha_1, \ldots, \alpha_n)$ a splitting field of f/F. If we write $f = (x-\alpha_1)g$, get $g \in F(\alpha_1)[x]$ and g has roots $\alpha_2, \ldots, \alpha_n$, so the splitting field of g over $F(\alpha_1)$ is L. By ind hyp, $[L:F(\alpha_1)] \leq (n-1)!$. Then $[L:F] = [L:F(\alpha_1)]\cdot[F(\alpha_1):F] \leq (n-1)!\,[F(\alpha_1):F]$
But $[F(\alpha_1):F] = \deg(m_{\alpha_1,F})$ and $f(\alpha_1) = 0$ so $[F(\alpha_1):F] \leq n$
$\Rightarrow [L:F] \leq n!$. $\square$

Note The bound is sharp ($\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}$ splits x^3-2) but not always realized ($\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ splits $(x^2-2)(x^2-3)$ and $4 < 4!$).

Uniqueness:

$$\begin{array}{ccc} L_1 & & L_2 \\ | & & | \\ F_1 & \xrightarrow[\varphi]{\cong} & F_2 \end{array}$$

L_1 = splitting field of $f_1 \in F[x]$

L_2 = — " — $f_2 \in F[x]$

where coeffs of f_2 are φ(coeffs f_1)

<u>Thm</u> $\exists$ iso $\overline{\varphi} : L_1 \to L_2$ with $\varphi = \overline{\varphi}|_{F_1}$.

Pf by ind'n on $n = \deg(f_1) = \deg(f_2)$. If $n=1$, $L_1 = F_1$, $L_2 = F_2$ and we can take $\overline{\varphi} = \varphi$. Now suppose $n > 1$. Then $L_1 = F(\alpha_1, \dots, \alpha_n)$ for α_i roots of f_1. Consider $F_1 \subseteq F_1(\alpha_1) \subseteq L_1$ where L_1 is a splitting field of $g_1 = f_1/(x-\alpha_1)$ over $F_1(\alpha_1)$.

<u>Step 1</u> Let $h_1 \in F_1[x]$ be min poly of α_1 $/F_1$. Then

$$F_1(\alpha_1) = F_1[\alpha_1] \cong F_1[x]/(h_1).$$
$$\alpha_1 \mapsto x + (h_1)$$

<u>Step 2</u> $\varphi : F_1 \cong F_2$ induces $\tilde{\varphi} : F_1[x] \cong F_2[x]$, $f_1 \mapsto f_2$, and $h_1 \mapsto h_2 := \tilde{\varphi}(h_1)$ irred factor of f_2. Roots of f_2 are $\beta_1, \dots, \beta_n \in L_2$ where β_1 is a root of h_2.

<u>Step 3</u> Get $L_2 / F_2(\beta_1) / F_2$ with L_2 splitting $g_2 = f_2/(x-\beta_1)$.

Then $F_2(\beta_1) = F_2[\beta_1] \cong F_2[x]/(h_2)$
$$\beta_1 \mapsto x + (h_2)$$

<u>Step 4</u> $\tilde{\varphi}$ induces $F_1[x]/(h_1) \cong F_2[x]/(h_2)$ so we get
$$x + (h_1) \mapsto x + (h_2)$$

$$\begin{array}{ccccccc} L_1 & & & & & & L_2 \\ | & & & & & & | \\ F_1(\alpha_1) & \cong & F_1[x]/(h_1) & \cong & F_2[x]/(h_2) & \cong & F_2(\beta_1) \\ | & & & & & & | \\ F_1 & & & \xrightarrow[\cong]{\varphi} & & & F_2 \end{array}$$

<u>Step 5</u> Degree of $L_1 / F_1(\alpha_1)$ is $n-1$ so ind hyp produces $L_1 \cong L_2$ fitting into the diagram. $\square$

<u>Cor</u> If L_1, L_2 are splitting fields of $f \in F[x]$, then there is an iso $L_1 \cong L_2$ which is the identity on F.

Pf Apply the thm to $id : F \to F$. $\square$

Prop Let L be a splitting field of $f \in F[x]$, and suppose $h \in F[x]$ is irreducible with roots $\alpha, \beta \in L$. Then $\exists$ field iso $\sigma : L \to L$ that is identity on F, takes $\alpha \mapsto \beta$.

Pf Have
$$\begin{tikzcd} F(\alpha) = F[\alpha] \arrow[rrr, bend right, "\varphi"'] & \cong F[x]/(h) & \cong F[\beta] & = F(\beta) \end{tikzcd}$$
$$\alpha \mapsto x + (h) \mapsfrom \beta$$
$$\alpha \mapsto \beta, \quad \text{id on } F$$

Use the diagram of splitting fields
$$\begin{tikzcd} L \arrow[r, dashed, "\tilde{\varphi}"] & L \\ F(\alpha) \arrow[u, dash] \arrow[r, "\cong", "\varphi"'] & F(\beta) \arrow[u, dash] \\ & F \arrow[ul, dash] \arrow[u, dash] \end{tikzcd}$$
$\tilde{\varphi}$ — from thm

$\square$

e.g. $L = \mathbb{Q}(\sqrt{2})$ is the splitting field of $x^2 - 2 \in \mathbb{Q}[x]$ which has roots $\pm\sqrt{2}$ so $\exists$ iso $\begin{array}{c} L \to L \\ \sqrt{2} \mapsto -\sqrt{2} \end{array}$, id on $\mathbb{Q}$.

Note Such σ is an elt of $\mathrm{Gal}(L/F)$, the Galois group of L/F.

Normal Extensions

Q Given L/F, how can we tell if L is the splitting field of some $f \in F[x]$?

Prop Let L be the splitting field of $f \in F[x]$, and let $g \in F[x]$ be irred. If g has one root in L, then g splits completely over L.

Pf WLOG, f, g are monic. Then $L = F(\alpha_1, \ldots, \alpha_n)$ where $f = (x - \alpha_1) \cdots (x - \alpha_n)$.

If $\beta \in L$ is a root of g, then g is the min'l poly of β / F since g is irred. & monic.

Have $L = F[\alpha_1, \ldots, \alpha_n]$ so $\beta = h(\alpha_1, \ldots, \alpha_n)$ for some $h \in F[x_1, \ldots, x_n]$.

Now consider $s(x) = \prod_{\sigma \in \Sigma_n} (x - h(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})) \in L[x]$.

Roots all in L, include β. Suffices to show $s \in F[x]$. TPS Why?

(B/c then $g | s$, s splits completely.)

Consider $s(x) = \prod_{\sigma \in \Sigma_n} (x - h(x_{\sigma(1)}, \dots, x_{\sigma(n)}))$ with coeffs in $F[x_1, \dots, x_n]$.

This is clearly symmetric in $x_1, \dots, x_n$, so its expansion is of the form
$$s(x) = \sum_{i=0}^{n!} p_i(x_1, \dots, x_n)\, x^i$$
where each $p_i \in F[x_1, \dots, x_n]^{\Sigma_n}$. Since the α_i are roots of $f \in F[x]$, get $p_i(\alpha_1, \dots, \alpha_n) \in F$, so $s(x) \in F[x]$. $\square$

e.g. $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field of any polynomial in $\mathbb{Q}[x]$:
$p_{\sqrt[3]{2}, \mathbb{Q}} = x^3 - 2$ is irred $/\mathbb{Q}$ but has roots $\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$.

Defn An alg extn L/F is normal if every irred poly in $F[x]$ that has a root in L splits completely over L.

Aside Perhaps "equitable" would be a better term, but we are stuck with "normal."

HW L/F normal iff $m_{\alpha,F}$ splits completely $\forall \alpha \in L$.

Thm Suppose L/F. Then L is the splitting field of some $f \in F[x]$ iff L/F is normal and finite.

Pf ($\Rightarrow$) Finite by $n!$ bound on degree, just proved normal.

($\Leftarrow$) L/F normal and finite. By finiteness, $L = F(\alpha_1, \dots, \alpha_m)$ where each α_i alg $/F$. Let $p_i = m_{\alpha_i, F} \in F[x]$, set $f = p_1 \cdots p_m$.

Claim L is the splitting field of f.

Clearly f splits completely since each p_i has root α_i in L and L/F normal. Let L' be the subfield of L gen'd by F and the roots of f. Then $L = F(\alpha_1, \dots, \alpha_m) \subseteq L' \subseteq L$ so $L' = L$, and L is the splitting field of f over F. $\square$

Separable Extensions

For $f \in F[x]$ and $\beta_1, \dots, \beta_r$ distinct in L/F s.t.

$$f = a_0 (x-\beta_1)^{m_1} \cdots (x-\beta_r)^{m_r} \quad , \quad a_0 \in F, \ m_1, \dots, m_r \geq 1$$

call m_i the multiplicity of β_i. Say β_i is a simple root if $m=1$ and a multiple root if $m_i > 1$.

Defn A poly $f \in F[x]$ is separable if it is nonconstant and its roots in a splitting field are all simple.

Slogan Separable = distinct roots

e.g. $x^2 - 2x + 1 = (x-1)^2$ is not separable

Recall discriminant $\Delta(f)$ of a monic $f \in F[x]$ of deg > 1:

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \quad \text{when } f = (x-\alpha_1)\cdots(x-\alpha_n)$$

Prop If $f \in F[x]$ is monic and nonconst, then TFAE:

(a) f is separable

(b) $\Delta(f) \neq 0$

(c) f and f' (the derivative of f) are relatively prime in $F[x]$.

Pf Trivially true if $\deg(f) = 1$ since $\Delta(f) = 1$ by convention in this case. Suppose $n = \deg(f) > 1$. (a) $\Leftrightarrow$ (b) clear. ~~Note that (a) ⇒ (c)~~

Let L be a splitting field of f/F so that $f = (x-\alpha_1)\cdots(x-\alpha_n) \in L[x]$.

For a given i, write $f(x) = (x-\alpha_i) h_i(x)$, so $h_i(x) = \prod_{j \neq i} (x - \alpha_j)$.

By the product rule, $f'(x) = (x-\alpha_i) h_i'(x) + h_i(x)$. Eval'n at α_i gives $f'(\alpha_i) = h_i(\alpha_i)$. If (c) is false, then f, f' have a common factor g of pos degree. Since $g | f$, $g(\alpha_i) = 0$ for some i, and then $g | f'$ implies $f'(\alpha_i) = 0$. Hence $0 = f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j)$

$\implies \alpha_i = \alpha_j$ for some $j \neq i$.

If (c) is true, then $1 = Af + Bf'$ for some $A, B \in F[X]$. Eval'n at α_i gives $1 = B(\alpha_i) f'(\alpha_i)$, so $f'(\alpha_i) \neq 0$, so $\prod_{j \neq i} (\alpha_i - \alpha_j) \neq 0 \ \forall i$
$\Rightarrow \alpha_1, \ldots, \alpha_n$ are distinct. $\square$

<u>Defn</u> For L/F an alg extn,

(a) $\alpha \in L$ is <u>separable</u> over F if $m_{\alpha,F}$ is sep $/F$;

(b) L/F is a <u>separable extension</u> if every $\alpha \in L$ is sep $/F$.

<u>Lemma</u> A nonconstant $f \in F[x]$ is separable iff f is a product of irred polys, each of which is separable and no two of which ~~is~~ are multiples of each other. $\square$

<u>Lemma</u> Let $f \in F[x]$ be an irred poly of degree n. Then f is separable if either of the following conditions is satisfied:

(a) F has characteristic 0, or

(b) F has char $p > 0$ and $p \nmid n$.

<u>Pf</u> Let $f = a_0 x^n + \cdots + a_{n-1} x + a_n$, $n > 0$, $a_0 \neq 0$. Then
$f' = n a_0 x^{n-1} + \cdots + a_{n-1}$. By (a) or (b), $n \neq 0 \in F$, so $a_0 \neq 0 \Rightarrow n a_0 \neq 0 \Rightarrow f' \neq 0$ of deg $n-1$. By irred of f, $\gcd(f, f') = 1$ or f. Deg of gcd $\leq n-1$, so in fact $= 1$. $\square$

<u>e.g.</u> $x^n - 1 \in F[x]$ is <u>nonseperable</u> iff $\mathrm{char}(F) = p \mid n$.

<u>Characteristic 0</u>

<u>Cor</u> If $\mathrm{char}(F) = 0$, then

(a) every irred in $F[x]$ is separable

(b) every alg extn of F is separable

(c) a nonconst $f \in F[x]$ is separable iff f is a product of irred polys, no two of which are multiples of each other. $\square$

<u>Prop</u> Let char $F = 0$, $f \in F[x]$ have fact'n $f = c g_1^{m_1} \cdots g_l^{m_l}$, $c \in F$, $g_i \in F[x]$ monic irred distinct. Then
$\frac{f}{\gcd(f, f')} = c g_1 \cdots g_l$ and $g_1 \cdots g_l$ is sep w/ same roots as f in a splitting field.

Pf Reading: pp 112–113.

e.g. $f = x^{11} - x^{10} + 2x^8 - 4x^7 + 3x^5 - 3x^4 + x^3 + 3x^2 - x - 1 \in \mathbb{Q}[x]$.

Then $\gcd(f,f') = x^6 - x^5 + x^3 - 2x^2 + 1$ (Euclidean algorithm) so

$\dfrac{f}{\gcd(f,f')} = x^5 + x^2 - x - 1$ is sep w/ same roots as f.

<u>Characteristic $p > 0$</u>

<u>Lemma</u> char $F = p > 0$, $\alpha, \beta \in F$, then $(\alpha+\beta)^p = \alpha^p + \beta^p$, $(\alpha-\beta)^p = \alpha^p - \beta^p$.

Pf Binomial thm + $p \mid \binom{p}{r}$ for $1 \le r \le p-1$. $\square$

$(\alpha\beta)^p = \alpha^p\beta^p$ so $\alpha \mapsto \alpha^p$ is a homomorphism called the Frobenius homomorphism

<u>HW Hint</u> Use this to think about $x^3 - t$ $/\mathbb{F}_3$.

$f = x^p - t \in F[x]$, $F = k(t)$, char $k = p$ is nonseparable and irred.

(Skipping §5.4: Thm of Primitive Element, which tells us that for infinite F, $L = F(\alpha_1, \dots, \alpha_n)$ w/ each α_i sep $/F$, $\exists \alpha \in L$ s.t. $L = F(\alpha)$. We may prove this later via Galois thy.)

The Galois Group

For $K, L / F$, a field hom over F is a hom $\varphi: K \to L$ s.t. $\varphi|_F = id_F$. Write

$$\begin{tikzcd} K \arrow[rr, "\varphi"] & & L \\ & F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

Defn The Galois group of L/F is

$$Gal(L/F) = \left\{ \begin{tikzcd} L \arrow[rr, "\sigma"] & & L \\ & F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd} \;\middle|\; \sigma \text{ is an isomorphism} \right\}$$

$= $ automorphisms of L/F.

Prop $Gal(L/F)$ is a group under composition.

Pf
- $\sigma, \tau \in Gal(L/F) \Rightarrow \sigma\tau = \sigma \circ \tau \in Gal(L/F)$
- $id_L \in Gal(L/F)$
- $\sigma \in Gal(L/F) \Rightarrow \sigma^{-1} \in Gal(L/F)$ $\square$

e.g. $\overline{(\ )} \in Gal(\mathbb{C}/\mathbb{R})$ so $C_2 \cong \langle \overline{(\ )} \rangle \leq Gal(\mathbb{C}/\mathbb{R})$
(In fact, $=$)

Lemma L/F finite, $\sigma \in Gal(L/F)$, $h \in F[x_1, \dots, x_n]$, $\beta_1, \dots, \beta_n \in L$ then $\sigma(h(\beta_1, \dots, \beta_n)) = h(\sigma(\beta_1), \dots, \sigma(\beta_n))$.

Pf σ preserves $+, \cdot$, fixes F. $\square$

Prop L/F finite, $\sigma \in Gal(L/F)$. Then

(a) If $h \in F[x]$ nonconst, $\alpha \in L$ root of h, then $\sigma(\alpha)$ is also a root of h lying in L.

(b) If $L = F(\alpha_1, \dots, \alpha_n)$, then σ is uniquely determined by its values on $\alpha_1, \dots, \alpha_n$.

Pf (a) $0 = \sigma(0) = \sigma(h(\alpha)) = h(\sigma(\alpha))$.

(b) Since L/F finite, $L = F[\alpha_1, \dots, \alpha_n]$, so $\beta \in L$ has $\beta = h(\alpha_1, \dots, \alpha_n)$ for some $h \in F[x_1, \dots, x_n]$. Then $\sigma(\beta) = \sigma(h(\alpha_1, \dots, \alpha_n)) = h(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$. $\square$

<u>Cor</u> If L/F is finite, then $\mathrm{Gal}(L/F)$ is finite.

<u>Pf</u> Since L/F is finite, $L = F(\alpha_1, \dots, \alpha_n)$ with α_i alg/F.

If $p_i = m_{\alpha_i, F}$, then for $\sigma \in \mathrm{Gal}(L/F)$ must have $\sigma(\alpha_i)$ a root of p_i, and there are at most $\deg(p_i)$ of these. Since σ is determined by the values $\sigma(\alpha_i)$, conclude that $|\mathrm{Gal}(L/F)| \leq \prod_{i=1}^{n} \deg(p_i) < \infty$. $\square$

<u>e.g.</u> $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$: $x^3 - 2$ only has one real root, $\sqrt[3]{2}$, and $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$,

so $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$.

<u>e.g.</u> $F = k(t)$, $\mathrm{char}(k) = p > 0$, L the splitting field of $f = x^p - t$. If $\alpha \in L$ a root of f, then $L = F(\alpha)$ and $f = (x-\alpha)^p$. Thus α is the only root of $f \Rightarrow \mathrm{Gal}(L/F) = 1$.

<u>e.g.</u> Roots of x^2+1 are $\pm i$, so $\langle \bar{\ } \rangle = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong C_2$.

<u>e.g.</u> $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong C_2$, gen'd by $a + b\sqrt{2} \mapsto a - b\sqrt{2}$.

<u>e.g.</u> $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. For $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, know $\sigma(\sqrt{2}) = \pm\sqrt{2}$, $\sigma(\sqrt{3}) = \pm\sqrt{3}$, so $|\mathrm{Gal}(L/\mathbb{Q})| \leq 4$. If $=4$, then $\mathrm{Gal}(L/\mathbb{Q}) \cong C_2 \times C_2$.

<u>Prop</u> If
$$\begin{tikzcd} L_1 \arrow[rr, "\varphi", "\cong"'] & & L_2 \\ & F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$
then $\mathrm{Gal}(L_1/F) \xrightarrow{\cong} \mathrm{Gal}(L_2/F)$, $\sigma \longmapsto \varphi\sigma\varphi^{-1}$. $\square$

<u>Defn</u> Let $f \in F[x]$. The <u>Galois group</u> <u>of f</u> over <u>F</u> is $\mathrm{Gal}(L/F)$ for L a splitting field of F.

(Well-defined up to isomorphism by Prop.)

<u>e.g.</u> $\mathrm{Gal}(x^2+1/\mathbb{R}) \cong \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong C_2$.

Galois groups of splitting fields

Thm Let L be the splitting field of $f \in F[x]$. Then

$|\mathrm{Gal}(L/F)| \le [L:F]$ with equality iff f is separable over F.

Pf by induction on $[L:F]$. If $[L:F]=1$, then $L=F$ and $\mathrm{Gal}(F/F)=1$ and has order 1. If $[L:F]>1$, then f has at least one irred factor p of $\deg > 1$. Let α be a fixed root of p and $\sigma \in \mathrm{Gal}(L/F)$.

Set $\tau = \sigma|_{F(\alpha)}$ and $\beta = \tau(\alpha)$, which is a root of p. We get

~~Claim~~ Conversely, for β any root of p, we ~~claim~~ know $\exists\ \tau : F(\alpha) \to F(\beta)$ extending id_F.

$$\begin{tikzcd}
L \arrow[r, "\sigma"] \arrow[d, dash] & L \arrow[d, dash] \\
F(\alpha) \arrow[r, "\tau"'] \arrow[dr, dash] & F(\beta) \arrow[d, dash] \\
 & F
\end{tikzcd}$$

~~Assuming the claim~~ Thus, we get an associated ext'n of τ to all of L.

Thus $|\mathrm{Gal}(L/F)| =$ ~~# distinct factors of f over L~~

$\prod$ # distinct factors over L of irred factors p_i of f over F

$\le \prod \deg(p_i)$ with equality iff f separable. $\square$

e.g. $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is the splitting field of the sep poly $(x^2-2)(x^2-3)$, so $|\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})| = 4$.

Note Splitting field & separable are necessary hypotheses for equality: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $k(t, \sqrt[p]{t})/k(t)$ for char $k=p$.

Defn L/F with L the splitting field of a separable polynomial is called a *Galois extension* of F.

Permutations of the roots

Assume L/F Galois for $f \in F[x]$. If $\deg(f)=n$, $f = a_0(x-\alpha_1)\cdots(x-\alpha_n)$ for $a_0 \ne 0 \in F$, α_i distinct elts of L.

Since $\sigma \in \mathrm{Gal}(L/F)$ permutes the roots α_i, we get a hom

$$\mathrm{Gal}(L/F) \longrightarrow \Sigma_n$$
$$\sigma \longmapsto \tau : \{1,\dots,n\} \to \{1,\dots,n\}$$
$$\text{where } \sigma(\alpha_i) = \alpha_{\tau(i)}.$$

(Every gp action $G \times S \to S$ gives a hom $G \to \Sigma_{|S|}$ in this way.)

Prop The hom $\mathrm{Gal}(L/F) \to \Sigma_n$ is injective.

Pf σ is determined by its action on $\alpha_1, \dots, \alpha_n$ so $\sigma = id_L$ iff $\sigma(\alpha_i) = \alpha_i \ \forall i$ iff $\sigma \mapsto 1$. $\square$

Cor If L is the splitting field of a sep poly $f \in F[x]$, then $[L:F] \mid n!$ for $n = \deg(f)$.

Pf May regard $\mathrm{Gal}(L/F) \le \Sigma_n$ by the prop, so this is implied by Lagrange's theorem. $\square$

Note Already proved $[L:F] \le n!$ (w/o separability hypothesis), so this refines that result.

e.g. $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $f = (x^2-2)(x^2-3)$

$\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\alpha_3 = \sqrt{3}$, $\alpha_4 = -\sqrt{3}$

Take $\sigma : \alpha_1 \leftrightarrow \alpha_2$, $\cancel{\alpha_3 \leftrightarrow \alpha_4}$ $\alpha_3 \circlearrowleft$ $\alpha_4 \circlearrowleft$

$\tau : \alpha_1 \circlearrowleft$ $\alpha_2 \circlearrowleft$ $\alpha_3 \leftrightarrow \alpha_4$

Get $\mathrm{Gal}(L/\mathbb{Q}) \cong \{e, (1\,2), (3\,4), (1\,2)(3\,4)\}$
$= \langle (1\,2), (3\,4) \rangle \le \Sigma_4$.

e.g. $L = \mathbb{Q}(\omega, \sqrt[3]{2})$ with $\omega = e^{2\pi i/3}$, splitting field of $x^3 - 2 / \mathbb{Q}$.

Have $\mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \Sigma_3$ and $|\mathrm{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] = 6$.

But $|\Sigma_3| = 6$, so $\mathrm{Gal}(L/\mathbb{Q}) \cong \Sigma_3$.

<u>Recall</u> A gp action $G \times S \to S$ is transitive if $\forall s,t \in S$ $\exists g \in G$ s.t. $gs = t$.

<u>Prop</u> Let L be the splitting field of sep $f \in F[x]$. Then $\mathrm{Gal}(L/F)$ acts transitively on the roots of f iff f is irred / F.

<u>Pf</u> We've already seen that f acts transitively on roots of irred factors of f. By separability, these sets are disjoint, and thus form the orbits of the action of $\mathrm{Gal}(L/F)$ on roots of f. Transitivity on all roots then corresponds to there being only 1 irred factor, i.e. f irred. $\square$

The p-th roots of 2 $\quad p$ prime

$\zeta_p = e^{2\pi i/p}$. The roots of $x^p - 2$ are $\zeta_p^j \sqrt[p]{2}$ for $0 \le j \le p-1$.

Thus $L = \mathbb{Q}(\sqrt[p]{2}, \zeta_p \sqrt[p]{2}, \zeta_p^2 \sqrt[p]{2}, \dots, \zeta_p^{p-1}\sqrt[p]{2})$

$\qquad = \mathbb{Q}(\zeta_p, \sqrt[p]{2})$

is the splitting field of $x^p - 2$ over $\mathbb{Q}$.

Min poly of ζ_p is $x^{p-1} + x^{p-2} + \dots + 1$ with roots ζ_p^i, $1 \le i \le p-1$.

Min poly of $\sqrt[p]{2}$ is $x^p - 2$ by Eisenstein criterion.

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\zeta_p) & & \mathbb{Q}(\sqrt[p]{2}) \\
 & \mathbb{Q} \arrow[ul, dash, "p-1"] \arrow[ur, dash, "p"'] &
\end{tikzcd}$$

Tower thm + $\gcd(p, p-1) = 1$

$\Rightarrow [L:\mathbb{Q}] = p(p-1)$.

Thus $|\mathrm{Gal}(L/\mathbb{Q})| = p(p-1)$. Take $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Then σ is determined by $\sigma(\zeta_p) \in \{\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\}$, $\sigma(\sqrt[p]{2}) \in \{\sqrt[p]{2}, \zeta_p\sqrt[p]{2}, \dots, \zeta_p^{p-1}\sqrt[p]{2}\}$.

Call $\sigma = \sigma_{i,j}$ if $\sigma(\zeta_p) = \zeta_p^i$, $\sigma(\sqrt[p]{2}) = \zeta_p^j \sqrt[p]{2}$

for some $1 \le i \le p-1$, $0 \le j \le p-1$. Every σ is of this form and there are only $(p-1)p$ choices for i,j, so all $\sigma_{i,j}$ are realized.

To determine group structure, we need to compute composition:

$$\sigma_{ij}\sigma_{rs}(\zeta) = \sigma_{ij}(\zeta^r) = (\sigma_{ij}\zeta)^r = \zeta^{ir}$$

$$\sigma_{ij}\sigma_{rs}(\sqrt[p]{2}) = \sigma_{ij}(\zeta^s \sqrt[p]{2}) = \sigma_{ij}(\zeta^s)\,\sigma_{ij}(\sqrt[p]{2}) = \zeta^{is}\zeta^j \sqrt[p]{2}$$

$$= \zeta^{is+j}\sqrt[p]{2}.$$

Thus $\sigma_{ij}\sigma_{rs} = \sigma_{ir,\, is+j}$ where the subscripts are interpreted in $\mathbb{F}_p$.

Get a bijection $\mathbb{F}_p^\times \times \mathbb{F}_p \longrightarrow \mathrm{Gal}(L/\mathbb{Q})$ but it's <u>not</u> a hom!

$$(i,j) \longmapsto \sigma_{ij}$$

Two perspectives on the group structure:

Geometry: Let $AGL_1(\mathbb{F}_p) = \{$ bij'ns $\mathbb{F}_p \to \mathbb{F}_p$ of the form $u \mapsto au+b$ for some $a,b \in \mathbb{F}_p\}$ — call this $\gamma_{a,b}$

Easy to check $\gamma_{a,b}$ bij iff $a \in \mathbb{F}_p^\times$.

Gp op is comp'n, and

$$\gamma_{a,b} \circ \gamma_{c,d}(u) = \gamma_{a,b}(cu+d) = a(cu+d)+b = acu+(ad+b)$$
$$= \gamma_{ac,ad+b}$$

Thus $\mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\cong} AGL_1(\mathbb{F}_p)$
$\sigma_{a,b} \longmapsto \gamma_{a,b}$.

Semi-direct product

① Recall that if $G = NH$ for $N \trianglelefteq G$, $H \leq G$, $N \cap H = 1$, then $G = N \rtimes H$, the semi-direct product of N & H.

② For $\varphi: H \to \mathrm{Aut}(N)$ hom, construct $N \rtimes_\varphi H$ with underlying set $N \times H$ and group op $(n_1,h_1)(n_2,h_2) = (n_1\varphi(h_1)(n_2), h_1h_2)$.

This recovers ① if $\varphi: h \mapsto (n \mapsto hnh^{-1})$ is the conjugation hom.

For $\mathrm{Gal}(L/F)$, take $N = \{\sigma_{1,j} \mid j \in \mathbb{F}_p\} \cong \mathbb{F}_p \cong C_p$. Note that $N \trianglelefteq \mathrm{Gal}(L/F)$. Take $H = \{\sigma_{i,0} \mid i \in \mathbb{F}_p^\times\} \cong \mathbb{F}_p^\times \cong C_{p-1}$.

Have $\sigma_{1,j}\sigma_{i,0} = \sigma_{1\cdot i, 1\cdot 0+j} = \sigma_{i,j}$ so $NH = \mathrm{Gal}(L/\mathbb{Q})$; clearly $N \cap H = 1$.

Finally compute $\sigma_{i0}\sigma_{1j}\sigma_{i0}^{-1} = (\sigma_{i\cdot 1, ij+0})\sigma_{i^{-1},0}$

$= \sigma_{i,ij}\sigma_{i,0}^{-1}$

$= \sigma_{1, i\cdot 0+ij}$

$= \sigma_{1,ij}$.

This corresponds to $\varphi: \mathbb{F}_p^\times \longrightarrow \mathrm{Aut}(\mathbb{F}_p)$
$i \longmapsto (j \mapsto ij)$, the mult by i map.

Get $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{F}_p \rtimes_{\mathrm{mult}_i} \mathbb{F}_p^\times$.

Galois Extensions

Defn For L/F finite and $H \leq \mathrm{Gal}(L/F)$,
$$L^H := \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$$
is the *fixed field* of H.

Moral Exc L^H is a field.

Thm L/F finite. TFAE:

(a) L is the splitting field of a separable polynomial in $F[x]$

(b) $F = L^{\mathrm{Gal}(L/F)}$

(c) L/F normal + separable.

Pf (a) $\Rightarrow$ (b): Let $K = L^{\mathrm{Gal}(L/F)}$. Clearly $L/K/F$, and the goal is to show $K = F$. Note L is also the splitting field of f over K, so $[L:F] = |\mathrm{Gal}(L/F)|$ & $[L:K] = |\mathrm{Gal}(L/K)|$. Also note $\mathrm{Gal}(L/K) \leq \mathrm{Gal}(L/F)$ since $\sigma|_K = id \Rightarrow \sigma|_F = id$. But $\mathrm{Gal}(L/F) \leq \mathrm{Gal}(L/K)$ as well b/c K is the fixed field of $\mathrm{Gal}(L/F)$. Thus $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/F)$ and $[L:F] = [L:K]$. Since $[L:F] = [L:K][K:F]$, we have $[K:F] = 1 \Rightarrow K = F$. ☺

(b) $\Rightarrow$ (c): Suppose $F = L^{\mathrm{Gal}(L/F)}$ and let $\alpha \in L$. Let $\{\alpha_1 = \alpha, \alpha_2, \dots, \alpha_r\} = \mathrm{Gal}(L/F) \cdot \{\alpha\}$. Consider $h(x) = \prod_{i=1}^{r} (x - \alpha_i) \in L[x]$.

Claim $h \in F[x]$ & h is irred $/F$.

Note that each $\sigma \in \mathrm{Gal}(L/F)$ permutes $\{\alpha_1, \dots, \alpha_r\}$, so it also permutes the factors $x - \alpha_i$ of h. Thus the coeffs of h are fixed by $\mathrm{Gal}(L/F) \Rightarrow h \in L^{\mathrm{Gal}(L/F)}[x] = F[x]$.

Next let $g \in F[x]$ be the irred factor of h vanishing at α. Then $\sigma(\alpha)$ is a root of g $\forall \sigma \in \mathrm{Gal}(L/F) \Rightarrow$ all α_i are roots of g, whence $h \mid g \Rightarrow h$ irred. ✓

Thus $h = m_{\alpha,F}$. Hence

- Normality: If $f \in F[x]$ irred w/ root $\alpha \in L$, then $f = ah$ for some $a \in F^\times$. Thus f splits completely over L, proving normality.

· Separability: If $\alpha \in L$, then its minimal poly is h. Then α sep since h is. ✓

(c) $\Rightarrow$ (a): Suppose L/F normal & sep. Then $L = F(\alpha_1, \dots, \alpha_n)$ where each $p_i = m_{\alpha_i, F}$ is sep. Let $q_1, \dots, q_r$ be the distinct elts of $\{p_1, \dots, p_n\}$, and set $f = q_1 \cdots q_r$. Then f is sep and L is the splitting field of f over F (check!). $\square$

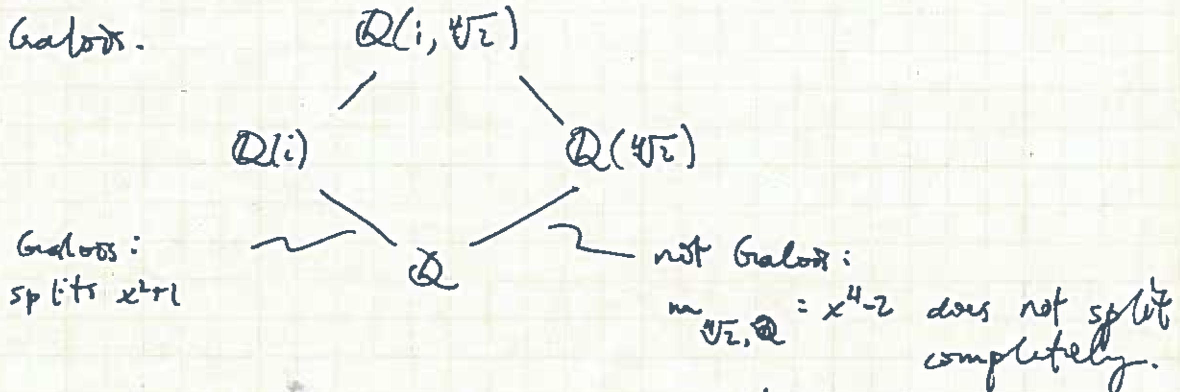
Defn An extn L/F is a Galois extn if it is finite and satisfies any of the equiv conditions of the Thm.

Note $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ Galois, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not.

Prop Suppose L/F is Galois and $L/K/F$ is a subextension. Then L/K is Galois.

Pf Use condition (a). $\square$

e.g. $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$ is the splitting field of $x^4 - 2$ and hence is Galois.



Thm Let L/F be finite. Then $|\mathrm{Gal}(L/F)| \mid [L:F]$.

Note Already proved $|\mathrm{Gal}(L/F)| \le [L:F]$ w/ equality iff L/F Galois.

Pf Let $K = L^{\mathrm{Gal}(L/F)}$. Then $L/K/F$ & $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/F)$. Thus $K = L^{\mathrm{Gal}(L/K)}$ so L/K is Galois. Hence

$$[L:F] = [L:K][K:F] = |\mathrm{Gal}(L/K)|\,[K:F] = |\mathrm{Gal}(L/F)|\,[K:F]. \quad \square$$

Finite separable extns

Prop L/F finite. L sep $/F$ iff $L = F(\alpha_1, \dots, \alpha_n)$ w/ each α_i sep $/F$.

Pf ($\Rightarrow$) ✓

($\Leftarrow$) Suppose $L = F(\alpha_1, \dots, \alpha_n)$ with each α_i sep $/F$. Let $p_i = m_{\alpha_i, F}$, and let $q_1, \dots, q_r$ be the distinct elts of $\{p_1, \dots, p_n\}$. Then $f = q_1 \cdots q_r$ is sep. Let M be the splitting field of f over L. Then $M = L(\beta_1, \dots, \beta_m)$ for β_i roots of f. Claim: $M = F(\beta_1, \dots, \beta_m)$. Clearly $\supseteq$. But the α_i are among the β_j, so $L = F(\alpha_1, \dots, \alpha_n) \subseteq F(\beta_1, \dots, \beta_m) \Rightarrow M \subseteq F(\beta_1, \dots, \beta_m)$, so equal. Thus M/F Galois and hence sep. Since $L \subseteq M$, every elt of L is sep. $/F$. $\square$

Galois closure

Prop If L/F finite sep, then M/L as above is Galois over F and is the smallest such extn of L.

Pf Reading (Prop 7.1.7). $\square$

Defn Call M as above the Galois closure of L/F.

Normal Subgroups / Normal Extensions

A. Conjugate Fields

Defn For finite extns $L/K/F$, $\sigma \in \mathrm{Gal}(L/F)$, call
$$\sigma K = \{\sigma(\alpha) \mid \alpha \in K\}$$
a *conjugate field of* K.

Note $[K:F] = [\sigma K : F]$ b/c

$$\begin{tikzcd} K \arrow[rr, "\sigma", "\cong"'] & & \sigma K \\ & F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

e.g. $\omega = e^{2\pi i/3}$

$$\begin{tikzcd} & & \mathbb{Q}(\omega, \sqrt[3]{2}) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\omega) & \mathbb{Q}(\sqrt[3]{2}) & \mathbb{Q}(\omega\sqrt[3]{2}) & \mathbb{Q}(\omega^2\sqrt[3]{2}) \\ & & \mathbb{Q} \arrow[ull, dash] \arrow[ul, dash] \arrow[u, dash] \arrow[ur, dash] & \end{tikzcd}$$

$\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$ is determined by $\sigma(\omega) \in \{\omega, \omega^2\}$ and $\sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$. It's easy to check that $\sigma\mathbb{Q}(\omega) = \mathbb{Q}(\omega)$ $\forall \sigma$. $\mathbb{Q}(\sqrt[3]{2})$ has $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\omega\sqrt[3]{2})$, $\mathbb{Q}(\omega^2\sqrt[3]{2})$ as its conjugates.

Lemma Finite extns $L/K/F$. Then

(a) $\mathrm{Gal}(L/K) \leq \mathrm{Gal}(L/F)$

(b) If $\sigma \in \mathrm{Gal}(L/F)$, then $\mathrm{Gal}(L/\sigma K) = \sigma \,\mathrm{Gal}(L/K)\, \sigma^{-1}$ in $\mathrm{Gal}(L/F)$.

Pf (a) ✓ since $F \subseteq K$.

(b) Let $\gamma \in \sigma \,\mathrm{Gal}(L/K)\, \sigma^{-1}$, $\beta \in \sigma K$. Then $\gamma = \sigma\tau\sigma^{-1}$ for some $\tau \in \mathrm{Gal}(L/K)$, and $\beta = \sigma(\alpha)$ for some $\alpha \in K$. Thus
$$\gamma(\beta) = \sigma\tau\sigma^{-1}(\sigma(\alpha)) = \sigma\tau(\alpha) = \sigma(\alpha) = \beta$$
$\Rightarrow \gamma|_{\sigma K} = id \Rightarrow \sigma \,\mathrm{Gal}(L/K)\, \sigma^{-1} \leq \mathrm{Gal}(L/\sigma K)$.

$\geq$ similar. $\square$

B. Normal subgps

Thm Suppose $L/K/F$ where L/F Galois. Then TFAE:

(a) $K = \sigma K$ $\forall \sigma \in Gal(L/F)$

(b) $Gal(L/K) \trianglelefteq Gal(L/F)$

(c) K/F Galois

(d) K/F normal.

Pf (a) $\Rightarrow$ (b): If $K = \sigma K$, then $Gal(L/K) = Gal(L/\sigma K) = \sigma Gal(L/K)\sigma^{-1}$ so $Gal(L/K) \trianglelefteq Gal(L/F)$.

(b)$\Rightarrow$(a): $Gal(L/K) \underset{\text{normality}}{=} \sigma Gal(L/K)\sigma^{-1} = Gal(L/\sigma K)$

L/K & $L/\sigma K$ Galois, so $K = L^{Gal(L/K)} = L^{Gal(L/\sigma K)} = \sigma K$.

(c) $\Rightarrow$ (d): ✓ as every Galois extn is normal and sep.

(d) $\Rightarrow$ (c): L/F Galois $\Rightarrow$ L/F sep $\Rightarrow$ K/F sep.

Thus K/F normal & sep, hence Galois.

(a)$\Rightarrow$ (d): Let $f \in F[x]$ be irred /F, root $\alpha \in K$. Then

$f = a_0 \prod_{i=1}^{r} (x - \alpha_i)$ for $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_r \in L$ distinct elts of L obtained by applying elts of $Gal(L/F)$ to α.

Since $\alpha \in K$, each $\alpha_i \in \sigma K = K \Rightarrow f$ splits completely over K.

(d) $\Rightarrow$ (a): Take $\alpha \in K$, $\sigma \in Gal(L/F)$, and let $p = m_{\alpha,F}$.

Then $\sigma(\alpha)$ is also a root of p. Since K/F is normal, p splits completely over $K \Rightarrow \sigma(\alpha) \in K \Rightarrow \sigma K \subseteq K$.

Since these fields have the same degree over F, $\sigma K = K$. $\square$

cf. Example 7.2.6 in Cox to see the implications of this theorem for $\mathbb{Q}(\omega,\sqrt[3]{2})/\mathbb{Q}$.

Thm Suppose $L/K/F$ with K/F & L/F Galois. Then $\mathrm{Gal}(L/K) \trianglelefteq \mathrm{Gal}(L/F)$ and $\mathrm{Gal}(L/F)/\mathrm{Gal}(L/K) \cong \mathrm{Gal}(K/F)$.

Pf If K/F Galois, then $\mathrm{Gal}(L/K) \trianglelefteq \mathrm{Gal}(L/F)$ by prev thm. For fixed $\sigma \in \mathrm{Gal}(L/F)$, $\sigma|_K : K \cong \sigma K = K \Rightarrow \sigma|_K$ an aut of K/F. Thus $\sigma \mapsto \sigma|_K$ defines $\Phi : \mathrm{Gal}(L/F) \to \mathrm{Gal}(K/F)$ which is clearly a homomorphism. Moreover,

$\sigma \in \ker\Phi \Leftrightarrow \sigma|_K = id_K \Leftrightarrow \sigma \in \mathrm{Gal}(L/K)$

$\therefore \ker\Phi = \mathrm{Gal}(L/K)$. It remains to show $\mathrm{im}\,\Phi = \mathrm{Gal}(K/F)$.

But
$$\begin{aligned}
|\mathrm{Im}\,\Phi| &= |\mathrm{Gal}(L/F)/\mathrm{Gal}(L/K)| \\
&= \frac{[L:F]}{[L:K]} \\
&= [K:F] \\
&= |\mathrm{Gal}(K/F)|
\end{aligned}$$

$\therefore \mathrm{im}\,\Phi = \mathrm{Gal}(K/F)$. $\square$

e.g.
$$\begin{array}{l}
L = \mathbb{Q}(\omega,\sqrt[3]{2}) \\
\quad | \langle\sigma\rangle \\
\mathbb{Q}(\omega) \\
\quad | \text{ Galois} \\
\mathbb{Q}
\end{array}
\Longrightarrow \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathrm{Gal}(L/\mathbb{Q})/\langle\sigma\rangle \cong \Sigma_3/A_3 \cong C_2.$$

Fundamental Thm of Galois Thy I

Let L/F be Galois.

(a) For $L/K/F$, $\mathrm{Gal}(L/K) \leq \mathrm{Gal}(L/F)$ has fixed field
$$L^{\mathrm{Gal}(L/K)} = K.$$
Furthermore $|\mathrm{Gal}(L/K)| = [L:K]$ and $[\mathrm{Gal}(L/F):\mathrm{Gal}(L/K)] = [K:F]$.

(b) For $H \leq \mathrm{Gal}(L/F)$, L^H has Galois gp
$$\mathrm{Gal}(L/L^H) = H.$$
Furthermore $[L:L^H] = |H|$ and $[L^H:F] = [\mathrm{Gal}(L/F):H]$.

Pf (a) L/K automatically Galois, so $L^{\mathrm{Gal}(L/K)} = K$.

$|\mathrm{Gal}(L/K)| = [L:K]$, $|\mathrm{Gal}(L/F)| = [L:F]$ since both extns Galois. Tower thm then gives
$$[\mathrm{Gal}(L/F):\mathrm{Gal}(L/K)] = \frac{[L:F]}{[L:K]} = [K:F].$$

(b) Take $H \leq \mathrm{Gal}(L/F)$. Then $L/L^H/F$, and $H \leq \mathrm{Gal}(L/L^H)$. L/L^H Galois, so
$$|H| \leq |\mathrm{Gal}(L/L^H)| = [L:L^H]$$

Thus it suffices to show equality. Suppose for contradiction that $|H| < [L:L^H]$. Then $\exists \alpha_1, \ldots, \alpha_{n+1} \in L$ which are L^H-lin ind. for $n = |H|$. Let $H = \{\sigma_1, \ldots, \sigma_n\}$. Then the system

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0 \\ &\vdots \\ \sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \cdots + \sigma_n(\alpha_{n+1})x_{n+1} &= 0 \end{aligned} \quad (*)$$

of n equations in $n+1$ unknowns $x_1, \ldots, x_{n+1}$ has a solution $x_1 = \beta_1, \ldots, x_{n+1} = \beta_{n+1}$ in L where not all $\beta_i = 0$. By lin ind of $\alpha_1, \ldots, \alpha_{n+1}$ (and $\sigma_1 = e$) not all β_i are in L^H.

Among all nontrivial sol'ns $(\beta_1, \ldots, \beta_{n})$ of ⊛, choose one with a minimal # of nonzero β_i. WLOG, $\beta_1, \ldots, \beta_r \neq 0$, and dividing by β_r, $\beta_r = 1$. Know that at least 1 of $\beta_1, \ldots, \beta_{r-1}, 1 \notin L^H$ (so $r > 1$), say $\beta_1 \notin L^H$. Then ⊛ becomes $\sigma_i(\alpha_1)\beta_1 + \cdots + \sigma_i(\alpha_{r-1})\beta_{r-1} + \sigma_i(\alpha_r) = 0$, $i = 1, \ldots, n$

Since $\beta_1 \notin L^H$, $\exists$ auto σ_{k_0} $(k_0 \in \{1, \ldots, n\})$ with $\sigma_{k_0}\beta_1 \neq \beta_1$.

Applying σ_{k_0}, get

$$\sigma_{k_0}\sigma_i(\alpha_1)\,\sigma_{k_0}(\beta_1) + \cdots + \sigma_{k_0}\sigma_i(\alpha_{r-1})\,\sigma_{k_0}(\beta_{r-1}) + \sigma_{k_0}\sigma_i(\alpha_r) = 0$$

for $i = 1, \ldots, n$. But $\{\sigma_{k_0}\sigma_i \mid i = 1, \ldots, n\} = H = \{\sigma_1, \ldots, \sigma_n\}$ so have

$$\sigma_i(\alpha_1)\,\sigma_{k_0}(\beta_1) + \cdots + \sigma_i(\alpha_{r-1})\,\sigma_{k_0}(\beta_{r-1}) + \sigma_i(\alpha_r) = 0$$

Subtracting systems, get

$$\sigma_i(\alpha_1)(\beta_1 - \sigma_{k_0}(\beta_1)) + \cdots + \sigma_i(\alpha_{r-1})(\beta_{r-1} - \sigma_{k_0}(\beta_{r-1})) = 0$$

for $i = 1, \ldots, n$. This is a sol'n of ⊛ with fewer nonzero "β_i" and it's nontrivial since $\beta_1 \neq \sigma_{k_0}\beta_1$. ☹

This proves $|H| = [L : L^H]$ and $\mathrm{Gal}(L/L^H) = H$.

$$\left.\begin{array}{c} L \\ \Big|\ {\scriptstyle |H|} \\ L^H \\ \Big| \\ F \end{array}\right\} |\mathrm{Gal}(L/F)| \implies [L^H : F] = \frac{|\mathrm{Gal}(L/F)|}{|H|} = [\mathrm{Gal}(L/F) : H].$$

$\square$

<u>FTGT II</u> L/F Galois. Then

$$\{K \mid L/K/F\} \xrightarrow{\cong} \{H \mid H \leq \mathrm{Gal}(L/F)\}$$

$$K \longmapsto \mathrm{Gal}(L/K)$$

$$L^H \longleftarrow\!\shortmid H$$

are inverses of each other which reverse inclusions.
Furthermore, if $K \mapsto H$ under this bij'n, then K/F is Galois iff $H \trianglelefteq \mathrm{Gal}(L/F)$, and when this happens, there is a natural isomorphism $\mathrm{Gal}(L/F)/H \cong \mathrm{Gal}(K/F)$.

Pf $K \longmapsto \mathrm{Gal}(L/K) \longmapsto L^{\mathrm{Gal}(L/K)} = K$ ✓

$H \longmapsto L^H \longmapsto \mathrm{Gal}(L/L^H) = H$ ✓

Inclusion-reversing is an easy check.

Normality portion proved Wednesday. $\square$

The splitting field of x^8-2

The splitting field of $x^8-2\,/\mathbb{Q}$ is gen'd by $\theta = \sqrt[8]{2} \in \mathbb{R}$ and $\zeta = \zeta_8 = e^{2\pi i/8}$.

Note that $i = \zeta_4 \in \mathbb{Q}(\zeta_8)$ and $\zeta_8 + \zeta_8^7 = \sqrt{2} \in \mathbb{Q}(\zeta_8)$

$\Rightarrow \mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$. In fact, $m_{\zeta,\mathbb{Q}} = x^4+1$

so $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$.

Since $\theta^4 = \sqrt{2}$, get that sp. field of x^8-2 is gen'd by θ, i.

$[\mathbb{Q}(\theta):\mathbb{Q}] = 8$ b/c θ has min'l poly x^8-2 (irred by Eisenstein).

$\mathbb{Q}(\theta) \subseteq \mathbb{R}$ so $i \notin \mathbb{Q}(\theta)$ so

$$\begin{array}{c} \mathbb{Q}(\theta,\zeta) = \mathbb{Q}(\theta, i) \\ \Big| \, 2 \\ \mathbb{Q}(\theta) \\ \Big| \, 8 \\ \mathbb{Q} \end{array} \qquad 16$$

The Galois gp is determined by its action on θ, i:

$$\begin{aligned} \theta &\longmapsto \zeta^a \theta \qquad a = 0, 1, \ldots, 7 \\ i &\longmapsto \pm i \end{aligned}$$

are possible, and there are only 16 of these, so they're all realized. Define

$$\sigma: \begin{cases} \theta \mapsto \zeta\theta \\ i \mapsto i \end{cases} \qquad \tau: \begin{cases} \theta \mapsto \theta \\ i \mapsto -i \end{cases}$$

Note that $\zeta = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} = \frac{1}{2}(1+i)\sqrt{2} = \frac{1}{2}(1+i)\theta^4$

Thus $\sigma(\zeta) = -\zeta = \zeta^5$, $\tau(\zeta) = \zeta^7$

Now compute:

f	$f(\theta)$	$f(i)$	$f(\zeta)$
σ	$\zeta\theta$	i	ζ^5
σ^2	$\zeta^6\theta$	i	ζ
σ^3	$\zeta^7\theta$	i	$-\zeta$
σ^4	$-\theta$	i	ζ
σ^5	$\zeta^5\theta$	i	$-\zeta$
σ^6	$\zeta^2\theta$	i	ζ
σ^7	$\zeta^3\theta$	i	$-\zeta$
τ	θ	$-i$	ζ^7
$\tau\sigma$	$\zeta^7\theta$	$-i$	ζ^3
$\tau\sigma^2$	$\zeta^2\theta$	$-i$	ζ^7
$\tau\sigma^3$	$\zeta\theta$	$-i$	ζ^3
$\tau\sigma^4$	$-\theta$	$-i$	ζ^7
$\tau\sigma^5$	$\zeta^3\theta$	$-i$	ζ^3
$\tau\sigma^6$	$\zeta^6\theta$	$-i$	ζ^7
$\tau\sigma^7$	$\zeta^5\theta$	$-i$	ζ^3

This exhausts the possibilities, (together with id) so σ, τ generate $\mathrm{Gal}(\mathbb{Q}(\theta,i)/\mathbb{Q})$

Clearly $\tau^2=1$, $(\sigma^4)^2=1$ so $\sigma^8=\tau^2=1$.

Also $\sigma\tau: \begin{cases}\theta \mapsto \zeta\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^3\end{cases}$

so $\sigma\tau=\tau\sigma^3$.

There are no other relns (why?) so

$\mathrm{Gal}(\mathbb{Q}(\theta,i)/\mathbb{Q})$

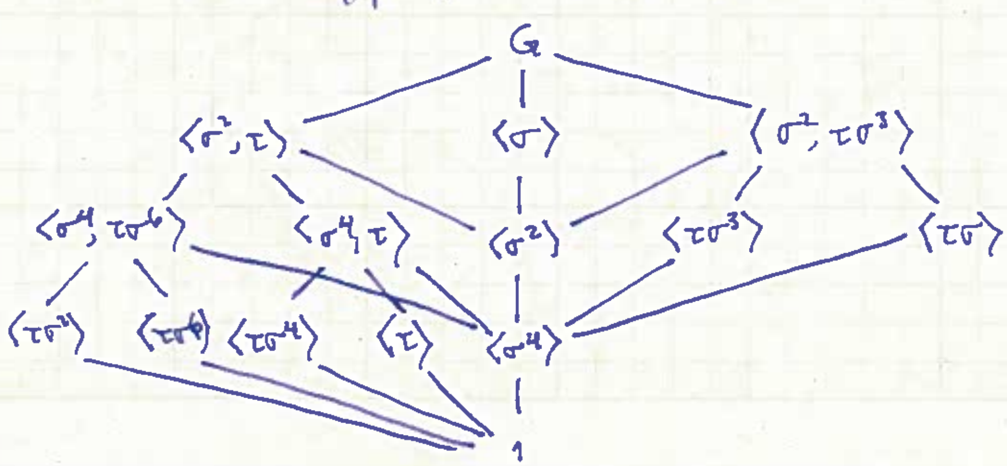
$=\langle \sigma,\tau \mid \sigma^8=\tau^2=1,\ \sigma\tau=\tau\sigma^3\rangle$

the <u>quasidihedral group</u> of order 16.

<u>TPS</u> Why can't θ,ζ be independently assigned?

<u>A</u> Algebraic dependence $\theta^4=\sqrt{2}=\zeta+\zeta^7$.

Lattice of subgps of $G=\mathrm{Gal}(\mathbb{Q}(\theta,i)/\mathbb{Q})$:

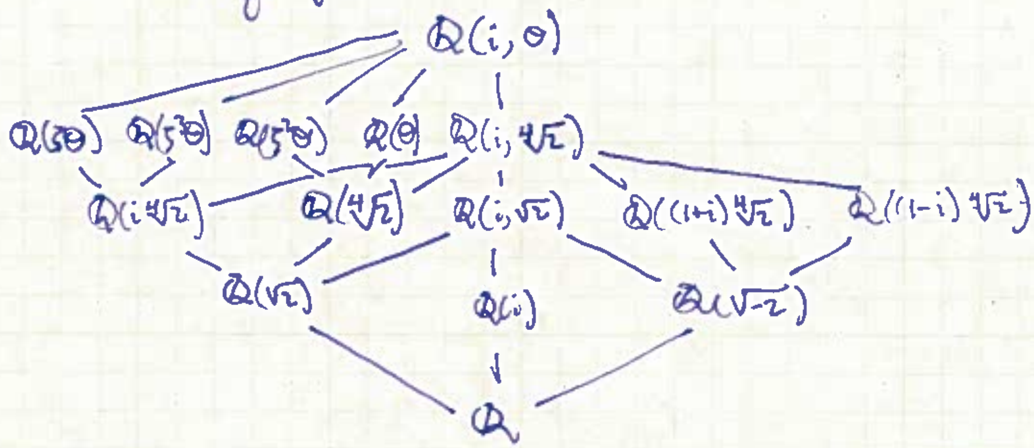


What is the corresponding lattice of subextensions?

For $\mathbb{Q}(\theta,i)/K/\mathbb{Q}$ with $K=\mathbb{Q}(\theta,i)^H$, $[K:\mathbb{Q}]=[G:H]$, so it suffices to find K of the correct degree fixed by (the generators of) H.

e.g. $\mathbb{Q}(i)$ is fixed by σ, $[G:\langle\sigma\rangle]=2$, and $[\mathbb{Q}(i):\mathbb{Q}]=2$, so $\mathbb{Q}(i)=\mathbb{Q}(\theta,i)^{\langle\sigma\rangle}$.

Ultimately get



e.g. $H=\langle\tau\sigma^3\rangle$. $\theta^2=\sqrt[4]{2}$ fixed by σ^4, $\langle\sigma^4\rangle \trianglelefteq H$ of index 2 with coset reps $1, \tau\sigma^3$. Consider

$$\alpha = (1+\tau\sigma^3)\theta^2 = \theta^2 + \tau\sigma^3\theta^2$$

$$\begin{aligned}\tau\sigma^3\alpha &= (\tau\sigma^3 + (\tau\sigma^3)^2)\theta^2 \\ &= (\tau\sigma^3+\sigma^4)\theta^2 \\ &= \alpha \quad \text{since } \sigma^4\theta^2=\theta^2\end{aligned}$$

Now $\alpha = \sqrt[4]{2} + i\sqrt[4]{2} = (1+i)\sqrt[4]{2} \in \mathbb{Q}(i,\theta)^H$.

Check $\sigma^2\alpha\neq\alpha$, so subgp diagram $\Rightarrow \mathbb{Q}(i,\theta)^H = \mathbb{Q}((1+i)\sqrt[4]{2})$.

Note $\tau H\tau^{-1} = \langle\tau\sigma\rangle$ has fixed field $\tau\mathbb{Q}(\alpha)=\mathbb{Q}(\tau\alpha)=\mathbb{Q}((1-i)\sqrt[4]{2})$.

The Discriminant

For a nonconstant monic $f \in F[x]$, have discriminant $\Delta(f) \in F$.

If $n = \deg(f) \geq 2$ and $f = (x-\alpha_1)\cdots(x-\alpha_n)$ in a splitting field L of f,

then $\Delta(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$ and f is seperable iff $\Delta(f) \neq 0$.

Define $\sqrt{\Delta(f)} = \prod_{i<j}(\alpha_i - \alpha_j) \in L$.

Recall that for f seperable, the action of $Gal(L/F)$ on roots $\{\alpha_1, \dots, \alpha_n\}$ determines $Gal(L/F) \hookrightarrow \Sigma_n$.

Thm Let f, L/F be as above and assume char $F \neq 2$.

(a) If $\sigma \in Gal(L/F) \longmapsto \tau \in \Sigma_n$, then
$$\sigma(\sqrt{\Delta(f)}) = sgn(\tau)\sqrt{\Delta(f)}.$$

(b) The image of $Gal(L/F)$ lies in the alternating group A_n iff $\sqrt{\Delta(f)} \in F$ (i.e. $\Delta(f) = a^2$ for some $a \in F$).

Pf Recall $\sqrt{\Delta} = \prod_{i<j}(x_i - x_j) \in F[x_1, \dots, x_n]$ has the property
$$\tau\sqrt{\Delta} = sgn(\tau)\sqrt{\Delta} \text{ for } \tau \in \Sigma_n.$$

Eval'n at $x_1 = \alpha_1, \dots, x_n = \alpha_n$ gives
$$\prod_{i<j}(\alpha_{\tau(i)} - \alpha_{\tau(j)}) = sgn(\tau)\prod_{i<j}(\alpha_i - \alpha_j) = sgn(\tau)\sqrt{\Delta(f)}$$

but $\sigma(\alpha_i) = \alpha_{\tau(i)}$ by defn, so the LHS $= \sigma(\sqrt{\Delta(f)})$. Thus (a).

For (b), L/F is Galois, so $F = L^{Gal(L/F)}$. Thus
$$\begin{aligned}\sqrt{\Delta(f)} \in F &\iff \sigma(\sqrt{\Delta(f)}) = \sqrt{\Delta(f)} \quad \forall \sigma \in Gal(L/F) \\ &\iff sgn(\tau)\sqrt{\Delta(f)} = \sqrt{\Delta(f)} \quad \forall \sigma \\ &\iff sgn(\tau) = 1 \quad \forall \sigma. \quad \square\end{aligned}$$

<u>Prop</u> Let $f \in F[x]$ be a monic irred sep cubic, char $F \neq 2$. If L is the splitting field of f over F, then

$$\mathrm{Gal}(L/F) \cong \begin{cases} C_3 & \text{if } \Delta(f) \text{ is a square in } F \\ \Sigma_3 & \text{o/w.} \end{cases}$$

<u>Pf</u> For α a root of F, $L/F(\alpha)/F$ and $[F(\alpha):F]=3$, so $[L:F]$ is a multiple of 3. We also have $\mathrm{Gal}(L/F) \hookrightarrow \Sigma_3$ and the only subgps of Σ_3 of order divisible by 3 are Σ_3 and $A_3 \cong C_3$. $\square$

<u>The Universal Extension</u>

$L = F(x_1, \dots, x_n) / K = F(\sigma_1, \dots, \sigma_n)$ for σ_i the elementary symm polys.

From reading: L is the splitting field of

$$\tilde{f} = x^n - \sigma_1 x^{n-1} + \dots + (-1)^n \sigma_n = \prod_{i=1}^{n} (x - x_i),$$

and $\mathrm{Gal}(L/K) \cong \Sigma_n$. Under this identification, $\sigma \in \Sigma_n$ permutes the x_i according to σ.

<u>Thm</u> Let $R \in F(x_1, \dots, x_n)$ be a rat'l fn.

(a) R is invariant under Σ_n iff $R \in F(\sigma_1, \dots, \sigma_n)$

(b) Assume char $F \neq 2$. Then R is invariant under A_n iff $\exists A, B \in F(\sigma_1, \dots, \sigma_n)$ s.t. $R = A + B\sqrt{\Delta}$.

<u>Pf</u> (a) $L^{\mathrm{Gal}(L/K)} = K$.

(b) Let $M = L^{A_n}$. Since $[\Sigma_n : A_n] = 2$, $[M:K] = 2$.

Since $\tau\sqrt{\Delta} = \mathrm{sgn}(\tau)\sqrt{\Delta}$, $\sqrt{\Delta} \in M$, so $K \subseteq K(\sqrt{\Delta}) \subseteq M$.

Thus $2 = [M:K] = [M:K(\sqrt{\Delta})][K(\sqrt{\Delta}):K]$. But $\sqrt{\Delta} \notin K$, so $K(\sqrt{\Delta}) = M$.

$\square$

Solvable Groups

<u>Defn</u> A finite group G is <u>solvable</u> if there are subgroups

$$1 = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G$$

s.t. for $i = 1, \ldots, n$ we have

(a) $G_i \trianglelefteq G_{i-1}$

(b) $[G_{i-1} : G_i]$ is prime. (so $G_i / G_{i-1} \cong C_p$)

<u>e.g.</u> · The chain $1 \leq A_3 \leq \Sigma_3$ exhibits Σ_3 as solvable.

· All finite abelian groups are solvable (soon).

· A_n, Σ_n are nonsolvable for $n \geq 5$ (later).

<u>Prop</u> Every subgp of a finite solvable gp is solvable.

<u>Pf</u> Let $\{G_i\}_{i=0}^n$ be a chain witnessing solvability of G.

For $H \leq G$ define $H_i = H \cap G_i$ and note $H_0 = H \cap G_0 = H \cap G = H$
$H_n = H \cap 1 = 1$.

Let π be the composite $H_{i-1} \hookrightarrow G_{i-1} \to G_{i-1}/G_i$.

Then $\ker \pi = \{ h \in H_{i-1} \mid hG_i = G_i \}$

$= H_{i-1} \cap G_i = (H \cap G_{i-1}) \cap G_i$

$= H \cap G_i = H_i \trianglelefteq H_{i-1}$.

By the first isomorphism thm,

$$H_{i-1}/H_i \cong \operatorname{im}(\pi) \leq G_{i-1}/G_i$$

so $H_{i-1}/H_i \cong 1$ or C_p.

$\Updownarrow$

$H_i = H_{i-1}$

So discarding duplicates we get a chain witnessing solvability of H. $\square$

<u>Thm</u> $H \trianglelefteq G$ finite. Then G is solvable iff H and G/H are solvable.

Pf First suppose G solvable. Then H is solvable by the prop. Let $\pi: G \to G/H$ be the quotient hom. and set $\tilde{G}_i = \pi(G_i)$. Exc After discarding duplicates, $\tilde{G}_i$ give a chain witnessing solvability of G/H.

Now suppose H, G/H solvable with

$$1 = H_\ell \leq H_{\ell-1} \leq \cdots \leq H_0 = H$$
$$1 = \tilde{G}_m \leq \cdots \leq \tilde{G}_0 = G/H$$

witnessing solvability. Then

$$1 = H_\ell \leq \cdots \leq H_0 = H \leq \pi^{-1}\tilde{G}_m \leq \cdots \leq \pi^{-1}\tilde{G}_0 = G$$

witnesses solvability of G. (check). $\square$

Prop Every finite abelian group G is solvable.

Pf by strong induction on $n = |G|$. The case $n=1$ is trivial. Assume G abelian of order $n > 1$ and the result is true $\forall$ abelian gps of order $< n$.

Let p be a prime divisor of n. If $p = n$, $G \cong C_p$ solvable. If $p < n$, Cauchy's thm says there is $\langle g \rangle \leq G$, $\langle g \rangle \cong C_p$. This is solvable & normal since G abelian. $|G/\langle g \rangle| < n$ so $G/\langle g \rangle$ solvable, so the prop follows from the theorem. $\square$.

e.g. $\mathbb{F}_p \cong T \trianglelefteq AGL_1(\mathbb{F}_p)$ with $AGL_1(\mathbb{F}_p)/T \cong \mathbb{F}_p^\times$. Both $\mathbb{F}_p, \mathbb{F}_p^\times$ abelian, hence solvable, so $AGL_1(\mathbb{F}_p)$ is solvable.

Rmk Feit-Thompson theorem: Every gp of odd order is solvable. Pf 255pp. $\square$

Radical & Solvable Extensions

<u>Defn</u> A field extension L/F is <u>radical</u> if there are fields
$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = L$ where for $i=1,\dots,n$ $\exists \gamma_i \in F_i$ s.t.
$F_i = F_{i-1}(\gamma_i)$ and $\gamma_i^{m_i} \in F_{i-1}$ for some integer $m_i > 0$.

Note if $b_i = \gamma_i^{m_i}$ then $F_i = F_{i-1}(\sqrt[m_i]{b_i})$, i.e. radical extns arise by adjoining successive radicals.

<u>e.g.</u> $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt{2+\sqrt{2}}) = \mathbb{Q}(\sqrt{2+\sqrt{2}})$
witnesses $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ as a radical extn.

<u>Defn</u> A field extn L/F is <u>solvable</u> (by radicals) if there is a field extn M/L s.t. M/F is radical.

<u>e.g.</u> The splitting field of x^3+x^2-2x+1 $/\mathbb{Q}$ is solvable but not radical.

<u>Defn</u> Suppose $K_1, K_2 \subseteq L$ subfields. The <u>compositum</u> K_1K_2 of K_1 & K_2 is the smallest subfield of L containing K_1, K_2.

$$\begin{tikzcd}[column sep=small] & L \arrow[d, dash] & \\ & K_1K_2 & \\ K_1 \arrow[uur, dash, bend left] & & K_2 \arrow[uul, dash, bend right] \end{tikzcd}$$

Existence: Fields are closed under arbitrary intersection.

<u>Prop</u> $M/L/F$ with M/F Galois. Then the compositum of all conjugate fields of L in M is the Galois closure of L/F.

<u>Lemma</u> $M/L_1, L_2/F$ with M/F Galois, then
~~$\mathrm{Gal}(L_1L_2/F) = \mathrm{Gal}(L_1/F) \cap \mathrm{Gal}(L_2/F)$~~
$\mathrm{Gal}(M/L_1L_2) = \mathrm{Gal}(M/L_1) \cap \mathrm{Gal}(M/L_2)$.

<u>Pf Lemma</u> If σ fixes L_1L_2 then it fixes L_1, L_2 so

$$\mathrm{Gal}(M/L_1L_2) \subseteq \mathrm{Gal}(M/L_1) \cap \mathrm{Gal}(M/L_2)$$

Suppose $\sigma \in \mathrm{Gal}(M/L_1) \cap \mathrm{Gal}(M/L_2)$. Suppose for ⨳ that $\sigma x \neq x$ for some $x \in L_1L_2$. Then $M^{\langle\sigma\rangle} \cap L_1L_2 \subsetneq L_1L_2$ with $L_1, L_2 \subseteq M^{\langle\sigma\rangle} \cap L_1L_2$, ⨳. $\square$

<u>Pf Prop</u> Compositum of the σL, $\sigma \in \mathrm{Gal}(M/F)$ has Galois gp $\bigcap_{\sigma \in \mathrm{Gal}(M/F)} \sigma \,\mathrm{Gal}(M/L)\, \sigma^{-1}$, which is clearly normal in $\mathrm{Gal}(M/F)$ so $\mathrm{Comp}_{\sigma \in \mathrm{Gal}(M/F)} (\sigma L) / F$ is Galois and contains ~~all Galois conjugates of~~ L. Now check that any Galois extn containing L contains all σL (exc). $\square$

<u>Properties of radical & solvable extns</u>

<u>Lemma</u> (a) If L/F, M/L are radical, so is M/F.

(b)

$$\begin{tikzcd}
& L \arrow[d, dash] & \\
& K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 \arrow[dr, dash, "\text{radical}"'] & & K_2 \arrow[dl, dash] \\
& F &
\end{tikzcd}
\implies K_1K_2/K_2 \text{ radical.}$$

(c) K_1/F, K_2/F radical $\implies K_1K_2/F$ radical

<u>Pf</u> (a) follows from defns & (c) $\Leftarrow$ (b).

For (b), the idea is to adjoin the same roots to K_2 (check details). $\square$

<u>Thm</u> If L/F is separable and radical, then the Galois closure of L is also radical.

<u>Pf</u> The Galois conjugates of L are radical. $\square$

<u>Cor</u> Solvable extns of char 0 fields have solvable Galois closure.

Solvable extensions, solvable groups.

<u>Assumption</u> All fields have char. 0.

For $m \in \mathbb{Z}^+$, field L, $x^m - 1$ is separable with roots $1, \zeta, \ldots, \zeta^{m-1}$ forming a cyclic group of order m. The splitting field is $L(\zeta)$, and $L(\zeta)/L$ is Galois and $\mathrm{Gal}(L(\zeta)/L)$ is Abelian. (Indeed, σ determined by $\sigma(\zeta) \in \{1, \ldots, \zeta^{m-1}\}$.)

Consider
$$\begin{tikzcd}[column sep=small] & L(\zeta) & \\ L \arrow[ur, dash] & & F(\zeta) \arrow[ul, dash] \\ & F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

<u>Lemma</u> If L/F is Galois, then $L(\zeta)/F$ and $L(\zeta)/F(\zeta)$ are also Galois, and
$$\begin{aligned} \mathrm{Gal}(L/F) \text{ is solvable} &\iff \mathrm{Gal}(L(\zeta)/F) \text{ is solvable} \\ &\iff \mathrm{Gal}(L(\zeta)/F(\zeta)) \text{ is solvable.} \end{aligned}$$

Pf Check $L(\zeta)/F$ Galois (exc), so $L(\zeta)/F(\zeta)$ is Galois as well.
For first equiv, get $\mathrm{Gal}(L(\zeta)/L) \trianglelefteq \mathrm{Gal}(L(\zeta)/F)$ with quotient $\cong \mathrm{Gal}(L/F)$.
$\uparrow$ Abelian, hence solvable.
Thus $\mathrm{Gal}(L(\zeta)/F)$ solvable $\iff \mathrm{Gal}(L/F)$ solvable. ✓
Similarly, $\mathrm{Gal}(F(\zeta)/F) \cong \mathrm{Gal}(L(\zeta)/F) / \mathrm{Gal}(L(\zeta)/F(\zeta))$.
$\uparrow$ Abelian, hence solvable, so $\mathrm{Gal}(L(\zeta)/F)$ solv $\iff$ solv. $\square$

<u>Lemma</u> Suppose M/K Galois with $\mathrm{Gal}(M/K) \cong C_p$, p prime. If K contains a primitive p-th root of unity ζ, then $\exists \alpha \in M$ s.t. $M = K(\alpha)$ and $\alpha^p \in K$.

Pf Later if time. Read on p. 203.

Thm L/F Galois. Then L/F solvable iff $\mathrm{Gal}(L/F)$ solvable

Pf ($\Rightarrow$) Reduce to the radical case:

$$\begin{tikzcd} M \arrow[d, dash] \\ L' \arrow[d, dash] \\ L \arrow[d, dash, "\text{solv}"] \\ F \end{tikzcd}$$

rad

Gal closure of L'/F is radical

Suppose $\mathrm{Gal}(M/F)$ solvable. Then $\mathrm{Gal}(L/F)$ is a solvable gp since it's isomorphic to $\mathrm{Gal}(M/F)/\mathrm{Gal}(M/L)$. Thus it suffices to show $\mathrm{Gal}(M/F)$ solvable, i.e. we may assume L/F radical and Galois.

If we adjoin a primitive m-th root of unity ζ to F and L, get $L(\zeta)/F(\zeta)$ radical and Galois. Showing $\mathrm{Gal}(L(\zeta)/F(\zeta))$ solvable will imply $\mathrm{Gal}(L/F)$ solvable. So WLOG, F contains any m-th root of unity we want.

Take $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{n-1} \subseteq F_n = L$ witnessing ~~s.t.~~ L/F radical: $F_i = F_{i-1}(\gamma_i)$ with $\gamma_i^{m_i} \in F_{i-1}$. May ~~as~~ assume F contains prim m_i-th root of unity, $i = 1, \ldots, n$. Claim F_i/F_{i-1} Galois with cyclic Galois group.

$\gamma_i, \zeta_i\gamma_i, \ldots, \zeta_i^{m_i-1}\gamma_i$ are the distinct roots of $x^{m_i} - \gamma_i^{m_i} \in F_{i-1}[x]$. Since $\zeta_i \in F \subseteq F_{i-1}$, we have $F_{i-1}(\gamma_i, \zeta_i\gamma_i, \ldots, \zeta_i^{m_i-1}\gamma_i) = F_{i-1}(\gamma_i) = F_i$, so F_i/F_{i-1} Galois. For $\sigma \in \mathrm{Gal}(F_i/F_{i-1})$, $\exists!\, 0 \le l \le m_i - 1$ s.t. $\sigma(\gamma_i) = \zeta_i^l \gamma_i$. For $C_{m_i} = \langle g \rangle$, $\sigma \mapsto g^l$ defines an injective hom $\mathrm{Gal}(F_i/F_{i-1}) \hookrightarrow C_{m_i}$. ~~$[F_i : F_{i-1}] = m_i$, so the~~ Thus $\mathrm{Gal}(F_i/F_{i-1})$ is cyclic.

Now prove $\mathrm{Gal}(L/F)$ solvable. Let $G_i = \mathrm{Gal}(L/F_i) \le \mathrm{Gal}(L/F)$. Get $1 = \mathrm{Gal}(L/L) = \mathrm{Gal}(L/F_n) = G_n \le G_{n-1} \le \cdots \le G_1 \le G_0 = \mathrm{Gal}(L/F)$

$$\begin{tikzcd} L \arrow[d, dash] \\ F_i \arrow[d, dash, "\text{Gal}"] \\ F_{i-1} \end{tikzcd}$$

Gal

$\Rightarrow G_i \trianglelefteq G_{i-1}$ with $G_{i-1}/G_i = \mathrm{Gal}(L/F_{i-1})/\mathrm{Gal}(L/F_i)$
$\cong \mathrm{Gal}(F_i/F_{i-1})$, cyclic hence Abelian.

Cor of G solv $\iff H, G/H$ solv is that filtration quotients solvable $\Rightarrow G$ solvable, so $\mathrm{Gal}(L/F)$ is solvable.

($\Leftarrow$) Let L/F be Galois with solvable Galois group.

Special case: F contains a primitive p-th root of unity $\forall$ prime $p \mid |\mathrm{Gal}(L/F)|$.

Now show L/F radical in this case: Take

$$1 = G_n \trianglelefteq \cdots \trianglelefteq G_0 = \mathrm{Gal}(L/F) \text{ witnessing solvability.}$$

Let $F_i = L^{G_i}$ to get

$$F = L^{\mathrm{Gal}(L/F)} = L^{G_0} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{n-1} \subseteq F_n = L^{G_n} = L^1 = L.$$

$G_i \trianglelefteq G_{i-1} \Rightarrow G_{i-1}/G_i \cong \mathrm{Gal}(F_i/F_{i-1}) \cong C_p$ for a prime p.

Exc $p \mid |\mathrm{Gal}(L/F)|$. The lemma implies $F_i = F_{i-1}(\alpha)$ for $\alpha^p \in F_{i-1}$. Thus L/F radical.

Now consider the general case:

Let $m = |\mathrm{Gal}(L/F)|$, ζ a prim m-th root of unity. Then $\mathrm{Gal}(L(\zeta)/F(\zeta))$ is solvable.

$$\mathrm{Gal}(L/F) \cong \mathrm{Gal}(L(\zeta)/F) / \mathrm{Gal}(L(\zeta)/L))$$

induced by

$$\begin{tikzcd} \mathrm{Gal}(L(\zeta)/F) \arrow[r, "\mathrm{res}_L"] & \mathrm{Gal}(L/F) \\ \mathrm{Gal}(L(\zeta)/F(\zeta)) \arrow[u, hook] \arrow[ur, "\mathrm{res}_L"'] & \end{tikzcd}$$

kernel b/c elts of ker are id on $LF(\zeta) = L(\zeta)$.

Thus $m = |\mathrm{Gal}(L(\zeta)/F(\zeta))| \mid \mathrm{Gal}(L/F)$. Take prime $p \mid m$. Then $\zeta^{m/p}$ is a primitive p-th root of unity, and $\zeta^{m/p} \in F(\zeta)$ so $L(\zeta)/F(\zeta)$ is in the special case, hence a radical extn. $F(\zeta)/F$ is radical, so $L(\zeta)/F$ is radical $\Rightarrow L/F$ solvable. $\square$

Cor L/F Galois of deg m, solvable, ζ a prim m-th root of 1. Then $L(\zeta)/F$ radical. $\square$

Pf Lemma Take $\langle\sigma\rangle = Gal(M/K) \cong C_p$. Fix $\beta \in M \setminus K$.

Then for $i = 0, \dots, p-1$, consider the Lagrange resolvent

$$\alpha_i = \beta + \zeta^{-i}\sigma(\beta) + \zeta^{-2i}\sigma^2(\beta) + \cdots + \zeta^{-i(p-1)}\sigma^{p-1}(\beta).$$

Then $\zeta^{-i}\sigma(\alpha_i) = \zeta^{-i}\sigma(\beta) + \zeta^{-2i}\sigma^2(\beta) + \cdots + \zeta^{-i(p-1)}\sigma^{p-1}(\beta) + \underbrace{\zeta^{-ip}\sigma^p(\beta)}_{\beta}$

$\Rightarrow \zeta^{-i}\sigma(\alpha_i) = \alpha_i$

$\Rightarrow \sigma(\alpha_i) = \zeta^i \alpha_i$

$\Rightarrow \sigma(\alpha_i^p) = \zeta^{ip}\alpha_i^p = \alpha_i^p$.

$\Rightarrow \alpha_i^p \in M^{Gal(M/K)} = K$. Also $\alpha_0 \in K$.

<u>Case 1</u> $\exists\, 1 \le i \le p-1$ s.t. $\alpha_i \ne 0$. Then $\zeta^i \ne 1$ so $\zeta^i\alpha_i \ne \alpha_i$

so $\sigma(\alpha_i) \ne \alpha_i$ so $\alpha_i \notin K$. Since $[M:K]$ prime, get

$M = K(\alpha_i)$ ✓

<u>Case 2</u> $\alpha_i = 0$ for $1 \le i \le p-1$. Then

$$\alpha_0 = \alpha_0 + \alpha_1 + \cdots + \alpha_{p-1}$$

$$= \cdots\cdots = p\beta.$$

So $\beta = \alpha_0/p$ & since $\alpha_0 \in K$, $\beta \notin K$. Thus we're always in case 1. $\square$

Simple Groups

Defn A group G is simple if its only normal subgroups are 1 and G.

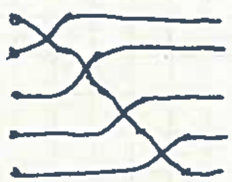
e.g. C_p for p prime (Lagrange's Thm)

Thm A_n is simple for $n \geq 5$.

Pf Two facts: ① l-cycle $(i_1 \cdots i_l) \in A_n$ iff l is odd

② For $n \geq 3$, A_n is gen'd by 3-cycles (HW)

For ①, $(i_1 \cdots i_l) = (i_1\ i_l) \cdots (i_1\ i_3)(i_1\ i_2)$.



Now suppose $H \neq 1 \trianglelefteq A_n$. Want to show $H = A_n$. First show H contains a 3-cycle. Take $1 \neq \sigma \in H$. Since $(j_1\ j_2\ j_3) \in A_n \trianglerighteq H$,

$$\sigma^{-1}(j_1\ j_2\ j_3)^{-1}\sigma\,(j_1\ j_2\ j_3) \in H.$$

If neither j nor $\sigma(j) \in \{j_1, j_2, j_3\}$, then $\sigma^{-1}(j_1\ j_2\ j_3)^{-1}\sigma(j_1\ j_2\ j_3)$ fixes j. Thus the elt in question moves at most 6 elts of $\{1, \ldots, n\}$.

Case 1 First suppose one of the cycles in σ has length ≥ 4, say $\sigma = (i_1\ i_2\ i_3\ i_4 \cdots)(\cdots)\cdots$. Then $\sigma^{-1}(i_2\ i_3\ i_4)^{-1}\sigma\,(i_2\ i_3\ i_4) = (i_1\ i_3\ i_4)$. Indeed, fixes all $j \notin \{i_1, i_2, i_3, i_4\}$ and $i_2 \mapsto i_3 \mapsto i_4 \mapsto i_3 \mapsto i_2$. Etc.

Case 2 Suppose σ has a 3-cycle. If σ is a 3-cycle, we're done. So may assume $\sigma = (i_1\ i_2\ i_3)(i_4\ i_5 \cdots)\cdots$.

Then $\sigma^{-1}(i_2\ i_3\ i_5)^{-1}\sigma\ (i_2\ i_3\ i_5) = (i_1\ i_4\ i_2\ i_3\ i_5)$

so H contains a 5-cycle, so, by Case 1, H contains a 3-cycle.

<u>Case 3</u> Finally suppose σ is a product of disjoint 2-cycles
$\sigma = (i_1\ i_2)(i_3\ i_4)\cdots$. Then $\sigma^{-1}(i_2\ i_3\ i_4)^{-1}\sigma\ (i_2\ i_3\ i_4)$
$= (i_1\ i_3)(i_2\ i_4) \in H$. Let i_5 be distinct from $i_1, \dots, i_4$
(using $n \geq 5$). Then

$$((i_1\ i_3)(i_2\ i_4))^{-1}(i_1\ i_3\ i_5)^{-1}((i_1\ i_3)(i_2\ i_4))(i_1\ i_3\ i_5)$$

$$= (i_1\ i_5\ i_3) \in H.$$

Now know some $(i\ j\ k) \in H$ and want to show all 3-cycles $\in H$.
Suppose i', j', k' distinct, and let $\theta \in \Sigma_n$ satisfy

$$\theta(i) = i',\quad \theta(j) = j',\quad \theta(k) = k'.$$

Then $\theta(i\ j\ k)\theta^{-1} = (i'\ j'\ k')$. If $\theta \in A_n$, get
$(i'\ j'\ k') \in H \trianglelefteq A_n$. If $\theta \notin A_n$, then $\theta' = \theta(i\ j) \in A_n$ and
$\theta'(i\ j\ k)\theta'^{-1} = (j'\ i'\ k') \in H$ so $(i'\ j'\ k') = (j'\ i'\ k')^{-1} \in H$.
As H contains all 3-cycles, $H = A_n$. $\square$

<u>Lemma</u> Let G be a nonabelian finite simple group. Then G is not solvable.

<u>Pf</u> Suppose $\cdots \trianglelefteq G_1 \trianglelefteq G_0 = G$ witnesses solvability. Then
$G_1 = 1$ by simplicity of G and $[G:G_1] = |G| = p$, prime.
But then $G = C_p$ is Abelian. $\square$

<u>Thm</u> A_n, Σ_n solvable iff $n \leq 4$.

Solving Polynomials by Radicals

* Assume all fields of char 0. *

Defn Let $f \in F[x]$ be nonconstant with splitting field L/F.

(a) A root $\alpha \in L$ of f is expressible by radicals over F if α lies in some radical extension of F.

(b) The polynomial f is solvable by radicals over F if L/F is a solvable extension.

Prop Let $f \in F[x]$ be irreducible. Then f is solvable by radicals over F iff f has a root expressible by radicals over F.

Pf $(\Rightarrow)$ ✓

$(\Leftarrow)$ Suppose $f(\alpha)=0$ with α in some radical extension of F. Then $F(\alpha)/F$ solvable, so its Galois closure M/F is solvable. By normality of M/F, M contains the splitting field of f over F so f is solvable by radicals. $\square$

Recall For $f \in F[x]$, $Gal(f/F) = Gal(L/F)$ for L a splitting field of f/F.

Thm A polynomial $f \in F[x]$ is solvable by radicals$/_F$ iff $Gal(f/F)$ is solvable. $\square$

Prop If $f \in F[x]$ has degree $n \leq 4$, then f is solvable by radicals.

Pf If f is separable, then $Gal(f/F) \leq \Sigma_4$ which is solvable. For the nonseparable case, work with nonrepeated irred factors of f. $\square$

e.g. $Gal(\underbrace{x^5-6x+3}_{\text{irreducible, so no root expressible by radicals!}} / \mathbb{Q}) \cong \Sigma_5$, not solvable.

· The Universal Polynomial:

$$\tilde{f} = x^2 - \sigma_1 x + \sigma_2 = (x-x_1)(x-x_2)$$

is solvable by radicals by the quadratic fmla.

Degree n generalization:

$$\tilde{f} = x^n - \sigma_1 x^{n-1} \cdots + (-1)^n \sigma_n = (x-x_1)\cdots(x-x_n)$$

solvable by radicals iff $L = F(x_1, \ldots, x_n) / F(\sigma_1, \ldots, \sigma_n) = K$ solvable iff $Gal(L/K) \cong \Sigma_n$ solvable. Hence have generic fmlae for roots iff $n \leq 4$.

Note Some polynomials of degree >4 are solvable by radicals.

· Abelian Equations:

Defn Let $f \in F[x]$. Call $f=0$ an Abelian equation if f separable with root α s.t. the roots of f are $\theta_1(\alpha), \ldots, \theta_n(\alpha)$ for $\theta_1, \ldots, \theta_n$ rational fns with coeffs in F satisfying

$$\theta_i(\theta_j(\alpha)) = \theta_j(\theta_i(\alpha)) \quad \forall i, j.$$

Thm Let $f \in F[x]$. If $f=0$ is an Abelian equation, then f is solvable by radicals over F.

Pf Abelian groups are solvable, so suffices to show $Gal(L/F)$ Abelian for L splitting field of f/F. For $\sigma, \tau \in Gal(L/F)$, check that

- $\sigma(\alpha) = \theta_i(\alpha)$, $\tau(\alpha) = \theta_j(\alpha)$ for some i, j.
- $\sigma\tau = \tau\sigma$ iff $\sigma(\tau(\alpha)) = \tau(\sigma(\alpha))$
- $\sigma(\tau(\alpha)) = \theta_j(\theta_i(\alpha))$ and $\tau(\sigma(\alpha)) = \theta_i(\theta_j(\alpha))$. $\square$

Thm Let $f \in F[x]$ be irred and separable of degree n with splitting field L/F. Then

$f = 0$ is Abelian iff $Gal(L/F)$ is Abelian.

When these conditions are satisfied, $|Gal(L/F)| = [L:F] = n$ and $L = F(\alpha)$ for any root $\alpha \in L$ of F.

Pf Just saw $\Rightarrow$. For $\Leftarrow$, let $\alpha \in L$ be a root of F. Then

$$L / F(\alpha) / F \longleftrightarrow Gal(L/F(\alpha)) \trianglelefteq Gal(L/F)$$

since $\uparrow$ Abelian.

Thus $F(\alpha)/F$ is Galois, so f splits completely in $F(\alpha)$ by normality. Thus $L = F(\alpha)$ and $[L:F] = n$. Each root is thus of the form $\theta_i(\alpha)$ for $\theta_i \in F(x)$. $\square$

Reading Thm 8.5.9: Artin's elegant proof of FTA.

It works for any extn C/R where R has no extns of odd degree >1, C has no extns of deg 2.

Cyclotomic Polynomials

Goal: Determine $\Phi_n := m_{e^{2\pi i/n},\mathbb{Q}}$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Defn The Euler ϕ-function $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$

$$n \longmapsto \left|\{i \mid 0 \le i < n,\ \gcd(i,n)=1\}\right|$$

Note: $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

Lemma (a) If $\gcd(n,m)=1$, then $\phi(nm) = \phi(n)\phi(m)$.

(b) If $n>1$, $\phi(n) = n \prod_{\substack{p\mid n \\ \text{prime}}} \left(1-\frac{1}{p}\right)$.

Pf (a) Assume $\gcd(n,m)=1$. Then Sun Zi's Thm implies

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

so $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$.

(b) For p prime, $\phi(p^a) = p^a - \left|\{j \mid 0 \le j < p^a,\ p \mid j\}\right|$

$$= p^a - \left|\{p\ell \mid 0 \le \ell < p^{a-1}\}\right|$$

$$= p^a - p^{a-1} = p^a\left(1-\frac{1}{p}\right).$$

So if $n = p_1^{a_1}\cdots p_s^{a_s}$ for p_i distinct primes, then

$$\phi(n) = \prod_{p_i \mid n} \phi(p_i^{a_i})$$

$$= n \prod_{p\mid n}\left(1-\frac{1}{p}\right). \quad \square$$

Let $\zeta = \zeta_n = e^{2\pi i/n}$. Then $x^n - 1 = \prod_{i=0}^{n-1}(x-\zeta^i)$. Define the <u>n-th cyclotomic polynomial</u> $\Phi_n(x) = \prod_{\substack{0\le i<n \\ \gcd(i,n)=1}} (x-\zeta^i)$.

Thus $\deg \Phi_n = \phi(n)$ and roots of Φ_n = primitive nth roots of 1 e.g. $\Phi_4 = (x-i)(x+i) = x^2+1$.

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

Prop $\Phi_n \in \mathbb{Z}[x]$ monic of deg $\phi(n)$. Furthermore,
$$x^n-1 = \prod_{d\mid n} \Phi_d(x)$$
where the product is over positive integers d dividing n.

Pf We have $x^n-1 = \prod_{0\le i<n}(x-\zeta^i) = \prod_{d\mid n}\prod_{\substack{0\le i<n \\ \gcd(i,n)=d}}(x-\zeta^i)$

If $\gcd(i,n)=d$, then $i=dj$ and $n=d\frac{n}{d}$ for $\gcd(j,\frac{n}{d})=1$.
Also $0\le i<n \iff 0\le dj < d\frac{n}{d} \iff 0\le j<\frac{n}{d}$
and $\zeta_n^d = \zeta_{n/d}$, so $x-\zeta_n^i = x-\zeta_n^{dj} = x-\zeta_{n/d}^j$

Thus $$\prod_{\substack{0\le i<n \\ \gcd(i,n)=d}}(x-\zeta^i) = \prod_{\substack{0\le j<\frac{n}{d} \\ \gcd(j,\frac{n}{d})=1}}(x-\zeta_{\frac{n}{d}}^j) = \Phi_{\frac{n}{d}}(x)$$

so $$x^n-1 = \prod_{d\mid n}\Phi_{\frac{n}{d}}(x) = \prod_{d\mid n}\Phi_d(x).$$

Now show $\Phi_n(x)\in\mathbb{Z}[x]$ by strong induction on n.
For $n=1$, $\Phi_1(x) = x-1\in\mathbb{Z}[x]$. If $n>1$,
$$x^n-1\ \cancel{\Phi_n(x)} = \Phi_n(x)\prod_{\substack{d\mid n \\ d<n}}\Phi_d(x) = \Phi_n(x)\underbrace{g(x)}_{\text{monic in }\mathbb{Z}[x]}$$
By the division algorithm, $\Phi_n(x)\in\mathbb{Z}[x]$. $\square$

Now compute $\underline{\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})}$.

Lemma $f\in\mathbb{Z}[x]$ monic of pos degree, p prime. If f_p is the monic polynomial whose roots are the p-th powers of the roots of f, then

$f_p \in \mathbb{Z}[x]$ and the coeffs of f, f_p are congruent mod p.

Pf Read lemma 9.1.8. (Play w/ symm polys)

Thm The cyclotomic polynomial $\Phi_n(x)$ is irred $/\mathbb{Q}$ so $\Phi_n = m_{\zeta_n,\mathbb{Q}}$ and $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \phi(n)$.

Pf Let $f \in \mathbb{Q}[x]$ be an irred factor of Φ_n. By Gauss's Lemma,

$\Phi_n = f \cdot g$ for $f, g \in \mathbb{Z}[x]$, monic.

Take p prime $\nmid n$. Step 1 $f(\zeta) = 0 \Rightarrow f(\zeta^p) = 0$.

Suppose for ⨳ $f(\zeta) = 0$ but $f(\zeta^p) \neq 0$. Take f as in lemma.

Ex 7 – HW: roots of f_p are distinct prim nth roots of 1.

Thus $f_p \mid \Phi_n$. If f, f_p share a root, then $f = f_p$

($f \mid f_p$ b/c f irred, have same degree). But this contradicts $f(\zeta^p) \neq 0$.

Thus f, f_p have no common roots so

$\Phi_n = f f_p h \Rightarrow h \in \mathbb{Z}[x]$ monic.

Let $\overline{(\ )} : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ reduce coeffs mod p. Since $\bar{f} = \bar{f}_p$ by the lemma, get $\bar{f}^2 \mid \bar{\Phi}_n \mid x^n - 1 \Rightarrow x^n - 1$ not separable in $\mathbb{F}_p[x]$. ⨳ since $p \nmid n$, completing Step 1.

Now let ζ be a fixed root of f, ζ' any prim nth root of 1.

HW: $\zeta' = \zeta_n^j$ for some $\gcd(j,n) = 1$. Let $j = p_1 \cdots p_r$ be prime fact'n.

Note each p_i rel prime n. By Step 1,

$$\zeta, \zeta^{p_1}, \zeta^{p_1 p_2}, \ldots, \zeta^{p_1 \cdots p_r} = \zeta^j$$

are roots of f. Thus every prim nth root of 1 is a root of $f \Rightarrow f = \Phi_n$.

Thm $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/n\mathbb{Z})^\times$

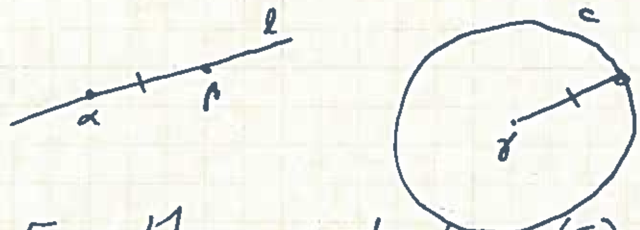
$\sigma \longmapsto [l]$ iff $\sigma(\zeta_n) = \zeta_n^l$. □

Constructible Numbers

What is a construction? Have some known points, use straightedge and compass to build lines and circles:

C1 From $\alpha \neq \beta$, can draw the line l through α, β.

C2 From $\alpha \neq \beta$ and γ, draw circle C with center γ and radius the distance from α to β.



From these constructions (C) get the following points

P1 The point of intersection of distinct lines l_1, l_2 constructed as above

P2 The points of intersection of a line l and circle C constructed as above

P3 The points of intersection of distinct circles C_1, C_2 constructed as above.

Consider the plane to be $\mathbb{C}$, start w/ #s/pts $0, 1$ to get

Defn $\alpha \in \mathbb{C}$ is constructible if there is a finite sequence of straightedge & compass constructions using C1, C2, P1, P2, P3 that begins w/ $0, 1$ and ends with α.

TPS Construct
- 2
- $n \in \mathbb{Z}$
- vertical axis
- $\pm i$, $\mathbb{Z}i$.

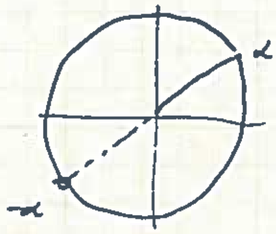
e.g. $\zeta_n = e^{2\pi i/n}$ constructible iff regular n-gon can be constructed by ruler and compass.

Thm $\mathcal{C} := \{\alpha \in \mathbb{C} \mid \alpha \text{ is constructible}\}$ is a subfield of $\mathbb{C}$. Furthermore

(a) Let $\alpha = a + ib$, $a, b \in \mathbb{R}$. Then $\alpha \in \mathcal{C}$ iff $a, b \in \mathcal{C}$.

(b) $\alpha \in \mathcal{C} \Longrightarrow \sqrt{\alpha} \in \mathcal{C}$.

Pf Take $\alpha \in \mathcal{C} \setminus 0$



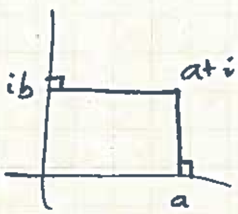
$\Longrightarrow -\alpha \in \mathcal{C}$

For $\alpha, \beta \in \mathcal{C}$ not collinear with 0

— intersect $|\beta|$ circle ~~thru~~ w/ center α with $|\alpha|$ circle ~~thru β~~ w/ center β.

Check collinear case.

This proves $\mathcal{C}$ is a subgp of $\mathbb{C}$ under $+$. Now prove (a):

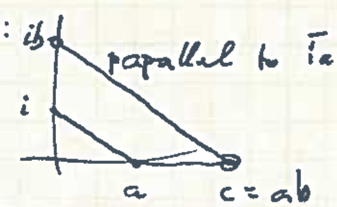


$a + ib \in \mathcal{C} \Longrightarrow a, ib \in \mathcal{C}$

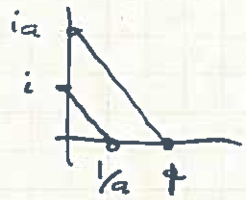
Circle w/ center 0 radius $|ib| = |b|$ gives $\pm|b|$, one of these is $b \in \mathcal{C}$.

Check $a, b \in \mathcal{C} \cap \mathbb{R} \Longrightarrow a + ib \in \mathcal{C}$. So (a) ✓

Now take $a, b \in \mathcal{C} \cap \mathbb{R}_{>0}$:



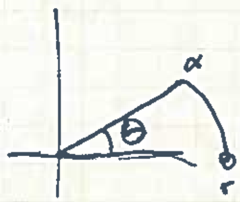
$\Longrightarrow ab \in \mathcal{C}$



$\Longrightarrow \frac{1}{a} \in \mathcal{C} \Longrightarrow \mathcal{C} \cap \mathbb{R}$ subfield of $\mathbb{R}$

$$\left.\begin{aligned} (a+ib)(c+id) &= (ac - bd) + i(ad + bc) \\ \frac{1}{a+ib} &= \frac{a}{a^2+b^2} + i\,\frac{-b}{a^2+b^2} \end{aligned}\right\} \Longrightarrow \mathcal{C} \text{ a field}$$

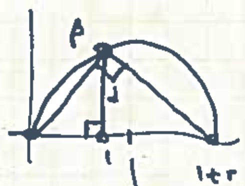
For (b), consider $\alpha = re^{i\theta}$, $r = |\alpha| > 0$, $\alpha \in C$.



angle bisection $\rightsquigarrow e^{i\frac{\theta}{2}}$ constr.

$r \Rightarrow r \in C$

So just need $\sqrt{r} \in C$:



$$\frac{1}{d} = \frac{d}{r} \Rightarrow d^2 = r \Rightarrow d = \sqrt{r} \in C.$$

$\square$

e.g. $\zeta_5 = \dfrac{-1+\sqrt{5}}{4} + \dfrac{i}{2}\sqrt{\dfrac{5+\sqrt{5}}{2}} \in C$ so the regular pentagon is constructible.

Thm For $\alpha \in \mathbb{C}$, $\alpha \in C$ iff $\exists$ subfields $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}$ with $\alpha \in F_n$ and $[F_i : F_{i-1}] = 2$ for $1 \le i \le n$.

<u>Thm</u> $\alpha \in C$ iff $\exists\, \mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{n-1} \subseteq F_n \subseteq \mathbb{C}$ s.t. $\alpha \in F_n$ and $[F_i : F_{i-1}] = 2$ for $1 \le i \le n$.

<u>Pf</u> ($\Leftarrow$) Have $F_i = F_{i-1}(\sqrt{\alpha_i})$ for some $\alpha_i \in F_{i-1}$. $F_0 = \mathbb{Q} \subseteq C$.

Suppose $F_{i-1} \subseteq C$. Then $\alpha_i \in C \Rightarrow \sqrt{\alpha_i} \in C$ so $F_i \subseteq C$. ✓

($\Rightarrow$) We show $\exists\, \mathbb{Q} = F_0 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}$ s.t. F_n contains $\mathrm{Re}(\alpha), \mathrm{Im}(\alpha)$ and $[F_i : F_{i-1}] = 2$. Then $\alpha \in F_n(i)$, so done.

Proceed by induction on N, number of times P1, P2, P3 used in construction of α. For $N=0$, $\alpha = 0$ or 1 so $F_n = F_0 = \mathbb{Q}$. Now suppose α constructed in $N > 1$ steps, where the last step uses P1, intersection of distinct lines l_1, l_2. Then l_1 constructed from α_1, β_1 by C1, l_2 from α_2, β_2 by C1. By ind hypothesis, $\exists\, \mathbb{Q} = F_0 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}$ with $[F_i : F_{i-1}] = 2$ and $F_n \ni \mathrm{Re}, \mathrm{Im}$ of $\alpha_1, \beta_1, \alpha_2, \beta_2$. Use linear algebra, line intersection fmla, to show $\mathrm{Re}(\alpha), \mathrm{Im}(\alpha) \in F_n$.

Next suppose last step in construction of α uses P2, intersection of line l, circle c. Then l built from $\alpha_1 \ne \beta_1$, C1 and c built from $\alpha_2 \ne \beta_2$ and γ_2, all coming from earlier stages of construction. Thus $\exists\, \mathbb{Q} = F_0 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}$ with $[F_i : F_{i-1}] = 2$ and F_n containing Re, Im of $\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_2$. Line/circle intersection is a quadratic cond'n and get $\underset{\mathrm{Re}, \mathrm{Im}(\ )}{\text{get}}$ $\alpha \in F_n$ or quad extn of F_n.

Sim for two circle intersections (P3) constructing α. $\square$

<u>Cor</u> C is the smallest subfield of $\mathbb{C}$ that is closed under the operation of taking square roots.

<u>Pf</u> Already showed $\alpha \in C \Rightarrow \sqrt{\alpha} \in C$. Take $F \subseteq \mathbb{C}$ closed under $\sqrt{\ }$ and take $z \in C$. Then $\exists\, \mathbb{Q} = F_0 \underset{2}{\subseteq} F_1 \underset{2}{\subseteq} \cdots \underset{2}{\subseteq} \underset{w}{F_n} \subseteq \mathbb{C}$

Same induction as before with F in place of C shows $F_n \subseteq F$ $\square$

Cor If $\alpha \in C$, then $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2^m$ for some $m \in \mathbb{N}$. Thus all $\alpha \in C$ are alg/$\mathbb{Q}$ with minimal poly /$\mathbb{Q}$ of degree 2^m.

e.g. You can't trisect a $120°$ angle b/c $\zeta_9 \notin C$. (HW)

e.g. Given a cube with volume 1, can we construct one with volume 2 ("duplication of the cube")?

Requires construction of $\sqrt[3]{2}$, but $\sqrt[3]{2}$ has min'l polynomial x^3-2 over $\mathbb{Q}$, so is not in C.

e.g. Given a radius 1 circle, can we construct a square of same area ("squaring the circle")?

Requires $\sqrt{\pi} \in C \Rightarrow (\sqrt{\pi})^2 = \pi \in C \Rightarrow \pi$ alg/$\mathbb{Q}$ $\lightning$.

Thm Let $\alpha \in C$ be alg /$\mathbb{Q}$ and let L be the splitting field of $m_{\alpha,\mathbb{Q}}$. Then α is constructible iff $[L:\mathbb{Q}]$ is a power of 2.

Note $L \neq \mathbb{Q}(\alpha)$ in general!

Pf Reading $\square$

Regular polygons and roots of unity:

Defn An odd prime p is a Fermat prime if $p = 2^{2^m}+1$ for some $m \geq 0$.

Thm Let $n>2$ be an integer. Then a regular n-gon can be constructed by straightedge + compass (i.e. $\zeta_n \in C$) iff $n = 2^s p_1 \cdots p_r$ where $s \geq 0$ is an integer and $p_1, \dots, p_r$ are distinct Fermat primes. $(r \geq 0)$.

Pf We have $\zeta_n \in C$ iff $[\mathbb{Q}(\zeta_n):\mathbb{Q}]$ is a power of 2, and $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \phi(n)$, so $\zeta_n \in C$ iff $\phi(n)$ is a power of 2.

Suppose $n = 2^s p_1 \cdots p_r$, p_i Fermat primes. Then

$$\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right) = \begin{cases} 2^{s-1}(p_1-1)\cdots(p_r-1) & \text{if } s>0 \\ (p_1-1)\cdots(p_r-1) & s=0 \end{cases}.$$

This is a power of 2 since each p_i is a Fermat prime.

Now suppose $\phi(n)$ is a power of 2 and $n = q_1^{a_1}\cdots q_s^{a_s}$ prime fact'n.

Then $\phi(n) = q_1^{a_1-1}(q_1-1)\cdots q_s^{a_s-1}(q_s-1)$

If q_i is odd, then $a_i = 1$ since $\phi(n)$ is a power of 2, and also $q_i - 1$ is a power of 2.

But if $q = 2^k+1$ is prime, then k is a power of 2 (HW).

So the odd q_i are Fermat primes and have $a_i = 1$. $\square$

Note $F_n = 2^{2^n}+1$ is prime for $n = 0, \dots, 4$, composite for $5 \le n \le 32$, unknown in gen'l.

n	F_n
0	3
1	5
2	17
3	257
4	65537

Finite Fields

Prop Let F be a finite field. Then

(a) $\exists!$ prime p s.t. F contains a subfield isomorphic to $\mathbb{F}_p$

(b) F is a finite extn of $\mathbb{F}_p$, and $|F| = p^n$ for $n = [F : \mathbb{F}_p]$.

Pf There is a unique ring hom $\mathbb{Z} \xrightarrow{f} F$ taking $1 \mapsto 1$. Since F is finite, the hom is not inj hence has kernel $m\mathbb{Z}$ for some $m > 1$, whence $\mathbb{Z}/m\mathbb{Z} \xrightarrow{\cong} \mathrm{im}(f)$. But $\mathrm{im}(f)$ has no 0 divisors, so in fact $m = p$ prime, and $\underbrace{\mathbb{Z}/p\mathbb{Z}}_{\mathbb{F}_p} \subseteq F$ by this map.

This makes F an $\mathbb{F}_p$-vs, and finiteness of $F \Rightarrow [F : \mathbb{F}_p] = n < \infty$.

But then $F \cong \mathbb{F}_p^n$ ~~as an~~ $\mathbb{F}_p$-vs, so $|F| = p^n$. $\square$

Thm Let F be a finite field with $q = p^n$ elements. Then

(a) $\alpha^q = \alpha \quad \forall \alpha \in F$

(b) $x^q - x = \prod_{\alpha \in F} (x - \alpha)$

(c) F is a splitting field over $\mathbb{F}_p$ of $x^q - x \in \mathbb{F}_p[x]$.

Thus any two fields with q elts are isomorphic.

Pf $F^\times$ ~~$\cong \mathbb{Z}_{q-1}$~~ is a group with $q-1$ elts, so $\alpha^{q-1} = 1 \ \forall \alpha \in F^\times$. So $\alpha^q = \alpha \ \forall \alpha \in F$. $\square$

Thm Given any prime p and any positive integer n, $\exists$ finite field with p^n elements.

Pf Let $q = p^n$ and let L be the splitting field of $x^q - x$ over $\mathbb{F}_p$. Then $x^q - x$ is separable, so $F = \{\alpha \in L \mid \alpha^q = \alpha\}$ is a subset of L containing q elts. F is a subfield (check) so is the desired field.

Prop If $f \in \mathbb{F}_p[x]$ is nonconstant and $n \geq 1$, then the number of roots of f in $\mathbb{F}_{p^n}$ is the degree of the polynomial $\gcd(f, x^{p^n} - x)$.

Pf Let $g = \gcd =$ product of the $x - \alpha_i$ dividing f (for $\mathbb{F}_{p^n} = \{\alpha_1, \dots, \alpha_{p^n}\}$).
But $x - \alpha_i$ divides f iff $f(\alpha_i) = 0$ so $g = \prod_{f(\alpha_i)=0} (x - \alpha_i)$. $\square$

Thm If $q = p^n$, then

(a) $\mathbb{F}_q / \mathbb{F}_p$ is a Galois extension of degree n.

(b) The map $\mathrm{Frob}_p : \mathbb{F}_q \to \mathbb{F}_q$, $\alpha \mapsto \alpha^p$ $\in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

(c) $\langle \mathrm{Frob}_p \rangle = \mathrm{Gal}(\mathbb{F}_q / \mathbb{F}_p) \cong C_n$

Pf $\mathbb{F}_q$ is the splitting field of the separable polynomial $x^q - x$.

$\mathrm{Frob}_p \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is obvious since $\mathbb{F}_q$ has char p and $a^p = a$ for $a \in \mathbb{F}_p$.

Know that the order of Frob_p divides n. Suppose $\mathrm{Frob}_p^r = \mathrm{id}$. Then $\alpha^{p^r} = \alpha$ $\forall \alpha \in \mathbb{F}_q$ $\Rightarrow$ $x^{p^r} - x$ has q roots in $\mathbb{F}_q$ $\Rightarrow$ $p^r = q$, so Frob_p has order n. $\square$

Cor For finite fields $\mathbb{F}_{p^m}, \mathbb{F}_{p^n}$, have $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ iff $m \mid n$.

Pf Suppose

$$\begin{tikzcd} \mathbb{F}_{p^n} \arrow[d, dash] \\ \mathbb{F}_{p^m} \arrow[d, dash, "m"] \\ \mathbb{F}_p \arrow[uu, bend left, dash, "n"] \end{tikzcd}$$

Then $m \mid n$ by the tower thm.

Conversely, suppose $m \mid n$. Since $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong C_n$, it has a subgp H of order $\frac{n}{m}$. Then $\mathbb{F}_{p^n}^H \cong \mathbb{F}_{p^m}$. $\square$

Thm For $m \mid n$, $\underbrace{\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})}_{= \langle \mathrm{Frob}_p^m \rangle} \cong C_{n/m}$. $\square$

Irreducible polynomials over finite fields.

<u>Prop</u> Let $f \in \mathbb{F}_p[x]$ be irred of deg m. Then
(a) $f \mid x^{p^n} - x$
(b) f is separable
(c) Given an integer $n \geq 1$, $f \mid x^{p^n} - x \iff f$ has a root in $\mathbb{F}_{p^n}$
$\iff m \mid n$.

<u>Pf</u> Begin with (c). Take α a root of f in the splitting field $\mathbb{F}_p$.
Since f irred, $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ has degree m, so $\mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^m}$.
Now $\mathbb{F}_{p^n} \supseteq \mathbb{F}_{p^m}$ iff $m \mid n$, so get second equivalence.
By irreducibility of f, $f \mid \gcd(f, x^{p^n} - x) \iff \deg(\gcd(f, x^{p^n}-x)) > 0$
and this degree $= \#$ roots of f in $\mathbb{F}_{p^n}$.
(a) & (b) follow easily. $\square$

<u>Note</u> In fact, ~~all~~ irred $f \in \mathbb{F}_q[x]$ are always separable.
Hence inseparability is only a phenomenon in infinite fields of char p.

Let $\mathcal{N}_m := \{f \in \mathbb{F}_p[x] \mid f \text{ is monic irred of degree } m\}$
$N_m := |\mathcal{N}_m|$.

<u>Thm</u> For $n \geq 1$, $\sum_{m \mid n} m N_m = p^n$.

<u>Pf</u> We have $x^{p^n} - x = \prod_{m \mid n} \prod_{f \in \mathcal{N}_m} f$ b/c the monic irred divisors of $x^{p^n} - x$ are exactly this collection of f by (c) above. Computing degrees on both sides (and $f \in \mathcal{N}_m$ has deg m) gives the Thm. $\square$

<u>e.g.</u> $N_1 = p$ so $p^2 = 2N_2 + N_1 = 2N_2 + p \Rightarrow N_2 = \frac{1}{2}(p^2 - p)$.
Sim, $N_4 = \frac{1}{4}(p^4 - p^2)$.

Recall $\mu(n) = \begin{cases} 1 & \text{if } n=1 \\ (-1)^s & \text{if } p = p_1 \cdots p_s,\ p_i \text{ distinct primes} \\ 0 & \text{o/w} \end{cases}$

Thm (Möbius inversion fmla) For $f, g : \mathbb{Z}^+ \to A$, A an Abelian gp, and $g(n) = \sum_{m|n} f(m)$, we have $f(n) = \sum_{m|n} \mu(m) g(n/m)$ (where operation on A is $+$).

Thm $N_n = \frac{1}{n} \sum_{m|n} \mu(m) p^{n/m}$.

Pf Let $f(n) = nN_n$. Then $g(n) = \sum_{m|n} f(m) = \sum_{m|n} m N_m = p^n$.

By Möbius inversion, $nN_n = \sum_{m|n} \mu(m) g(n/m) = \sum_{m|n} \mu(m) p^{n/m}$. □

e.g. $N_4 = \frac{1}{4}\left(\mu(1) p^{4/1} + \mu(2) p^{4/2} + \mu(4) p^{4/4}\right)$
$= \frac{1}{4}(p^4 - p^2)$.

Further directions:

- Irred factors of mod p reduction of Φ_d
- Berlekamp's algorithm: When is $f \in \mathbb{F}_p[x]$ irreducible

  } Reading

- Number theory: $K/\mathbb{Q}$ finite, $\mathcal{O}_K \subseteq K$ ring of integers,

  $\mathcal{O}_K / \mathfrak{m} \cong \mathbb{F}_q$

- Matrix groups $/\mathbb{F}_q \rightsquigarrow$ finite simple groups
- Coding theory: error correcting codes
- Cryptography via elliptic curves over finite fields

Combinatorics $\binom{n}{k}_q := \dfrac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}$

$q \to 1 : \binom{n}{k}$

$q = p^n$: # k-dim subspaces of $\mathbb{F}_q^n$

{ Field with one element? $\mathbb{F}_1$

Aside on Möbius inversion

Suppose $f, g : \mathbb{Z}^+ \to (A,+)$ for A an Abelian group.
~~Then~~ If $g(n) = \sum_{d|n} f(d)$, then $f(n) = \sum_{m|n} \mu(m)\, g(n/m)$

Pf We have

$$\sum_{d|n} \mu(d)\, g(n/d) = \sum_{d|n} \mu(n/d)\, g(d)$$

$$= \sum_{d|n} \mu(n/d) \Big(\sum_{d_1|d} f(d_1) \Big)$$

$$= \sum_{d_1|n} f(d_1) \Big(\sum_{d_1|d|n} \mu(n/d) \Big)$$

$$= \sum_{d_1|n} f(d_1) \underbrace{\Big(\sum_{d_2|m} \mu(m/d_2) \Big)}_{=1 \text{ for } m=1;\ o/w\ 0,\ \text{i.e. } d_1 = n}$$

where $m = \frac{n}{d_1}$, $d_2 = \frac{d}{d_1}$

$$= f(n).$$

$\square$

Formally Real Fields

Defn A field F is *formally real* if -1 is not a sum of squares in F; otherwise, F is called *nonreal*.

Notation $F^{\square} := \{a^2 \mid a \in F\}$

$F^{\blacksquare} := \{a^2 \mid a \in F^{\times}\} = F^{\square} \setminus \{0\}$.

$\sigma(F) = \{\sum_{i=1}^{n} a_i^2 \mid a_i \in F, n \in \mathbb{N}\}$

$\dot{\sigma}(F) = \sigma(F) \setminus \{0\}$

Note Formally real fields have char 0 b/c $\sigma(\mathbb{F}_p) = \mathbb{F}_p$ (check).

Prop (a) $\dot{\sigma}(F) \leq F^{\times}$

(b) If F is nonreal and char $F \neq 2$, then $\sigma(F) = F$.

Note If char $F = 2$, $\sigma(F) = F^{\square}$.

Pf (a) Easy to check closure of $\dot{\sigma}(F)$ under mult'n.

If $0 \neq a = a_1^2 + \cdots + a_n^2 \in F$, then

$$\frac{1}{a} = \frac{a}{a^2} = \left(\frac{a_1}{a}\right)^2 + \cdots + \left(\frac{a_n}{a}\right)^2 \in \dot{\sigma}(F).$$

(b) Given $x \in F$, we have $x = \left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2 \in F^{\square} + \sigma(F)F^{\square} \subseteq \sigma(F)$. $\square$

Defn An *ordering* on F is a set $P \subsetneq F$ called the *positive cone* of the ordering s.t.

(1) $P + P \subseteq P$

(2) $P \cdot P \subseteq P$

(3) $P \cup (-P) = F$.

Prop Let (F, P) be any ordered field. Then

(1) $\sigma(F) \subseteq P$

(2) $-1 \notin P$, and $P \cap (-P) = \{0\}$

(3) F is formally real

(4) $P^{\times} := P \setminus \{0\}$ is a subgp of index 2 in $F^{\times}$.

(5) If $P' \subsetneq F$ is another ordering, $P \subseteq P' \Rightarrow P = P'$

Pf Moral exc. Note (2) follows from same trick as (b) above, and (2) $\Rightarrow$ (3). $\square$

Note
- $F = P^\times \sqcup \{0\} \sqcup (-P^\times)$ so we can define a relation $\leq_P$ on F by $x \leq_P y$ iff $y - x \in P$. Get that $\leq_P$ is a total ordering on F.
- For F/F_0 and $P \subsetneq F$ an ordering, get an induced ordering $P_0 := F_0 \cap P$ on F_0
- $\mathbb{R}$ has a unique ordering by $\mathbb{R}^\square = \sigma(\mathbb{R}) = \mathbb{R}_{\geq 0}$.

Lemma Let F be formally real and $K = F(\sqrt{a})$ be a quadratic extn of F. Then K is nonreal iff $a \in \dot{\sigma}(F)$.

Pf If $-a \in \dot{\sigma}(F)$, then $(\sqrt{a})^2 + (-a) = 0$ shows that K is nonreal.

Conversely, if K is nonreal, have $-1 = \sum (b_i + c_i\sqrt{a})^2$, $b_i, c_i \in F$.

So $-1 = \sum b_i^2 + a \sum c_i^2$. Now $\sum c_i^2 \neq 0$ (o/w $-1 = \sum b_i^2 \in \sigma(F)$)

so $-a = \dfrac{1 + \sum b_i^2}{\sum c_i^2} \in \dot{\sigma}(F)$. $\square$

Defn F is Euclidean if F is formally real and $[F^\times : F^{\boxtimes}] = 2$.

Defn F is Pythagorean if the sum of two squares is always a square.

Prop If F is Euclidean, then F is Pythagorean with a unique ordering.

Note Converse is also true.

Pf Claim $P = F^\square$ is an ordering. Clearly have $P \subsetneq F$, $P \cdot P \subseteq F$, $P \cup (-P) = F$, so only need to show $P + P \subseteq P$, i.e. F is Pythagorean. Suffices to show $1 + y^2 \in F^{\boxtimes}$ for all $y \in F$. If $1 + y^2 \in F \setminus F^{\boxtimes} = -F^\square$, then $-1 \in \sigma(F)$ $\Rightarrow\Leftarrow$.

Uniqueness follows since $F^{\square} \subseteq \sigma(F) \subseteq P$ for all orderings. $\square$

<u>Thm</u> For all fields F, TFAE:

(1) F is Euclidean.

(2) F is formally real, but every quadratic extension of F is nonreal.

(3) $\sqrt{-1} \notin F$ and $K := F(\sqrt{-1})$ is quadratically closed (i.e. $K^{\square} = K$)

(4) $\text{char}(F) \neq 2$ and $\exists$ quad extn L/F that is quadratically closed.

<u>Pf</u> $(2) \Rightarrow (1)$: For any nonsquare $a \in F$, $F(\sqrt{a})$ is nonreal, so $-a = a_1^2 + \cdots + a_n^2$ for some $a_i \in F$. Take such an eqn with n minimal (so $a_i \neq 0$, in particular). Need to show $n=1$. If $n \geq 2$, $a_1^2 + a_2^2 \notin F^{\square}$ implies $-(a_1^2+a_2^2) = b_1^2 + \cdots + b_m^2$ for some $b_j \in F$, and this contradicts formal reality of F.

$(1) \Rightarrow (3) \Rightarrow (4) \Rightarrow (2)$: More work (norms, quadratic forms). $\square$

<u>Defn</u> A field F is <u>real closed</u> if F is formally real, but no proper algebraic extn of F is formally real.

<u>Cor</u> If F is real closed, then F is euclidean, has unique ordering $F^{\square}$, and $F(\sqrt{-1})$ is quadratically closed.

<u>Prop</u> Let F be a formally real field, and $\bar{F}$ its algebraic closure. Then $\exists$ real closed field R, $F \subseteq R \subseteq \bar{F}$.

<u>Pf</u> Let $\mathcal{R} = \{ L \subseteq \bar{F} \mid F \subseteq L,\ L \text{ formally real} \}$. If $\{F_\alpha\}$ is a chain in $\mathcal{R}$, then $\bigcup_\alpha F_\alpha \in \mathcal{R}$ too. By Zorn's Lemma, $\exists R \in \mathcal{R}$ that is maximal and thus real closed. $\square$

<u>Thm</u> F is formally real iff F has at least one ordering.

Pf. $\Leftarrow$: $-1 \notin P \supseteq \sigma(F)$.

$\Rightarrow$: Have an alg. extn $R \supseteq F$ that is real closed.

The unique ordering $R^{\square}$ on R induces one on F. $\square$

Fact Let $X_F = \{\text{orderings on } F\}$. Then $\bigcap_{P \in X_F} P = \sigma(F)$.

Say that the totally positive elts of F are the sums of squares.

e.g. $\mathbb{Q}(\sqrt{2}) \xrightarrow{\varphi} \mathbb{R}$, $\sqrt{2} \mapsto \sqrt{2}$; $\mathbb{Q}(\sqrt{2}) \xrightarrow{\varphi'} \mathbb{R}$, $\sqrt{2} \mapsto -\sqrt{2}$ induces two different orderings P, P' on $\mathbb{Q}(\sqrt{2})$. These are in fact the only two. ~~Since~~ For $\theta = 5+3\sqrt{2}$, have $\varphi(\theta), \varphi'(\theta) > 0$, so $5+3\sqrt{2} \in \sigma(\mathbb{Q}(\sqrt{2}))$.

In fact, $2(5+3\sqrt{2}) = 1^2 + (1+\sqrt{2})^2 + (1+\sqrt{2})^2 + (1+\sqrt{2})^2$.

e.g. Infinitely many orderings on $F(x)$ for F formally real.

Characterizations of real closed fields

Prop TFAE: (1) Any odd degree $f \in F[x]$ has a root in F
(2) F has no proper odd degree extns.

Pf (2) $\Rightarrow$ (1): By induction on $n = \deg(f)$. Triv for $n=1$. Assume $n>1$. If f is irred, then $F[x]/(f)$ proper odd deg extn, ⨳. So $f = f_1 f_2$ with, say, $\deg(f_1)$ odd $< n$. But then f_1 has a root in F so f does too.

(1) $\Rightarrow$ (2): If K/F has odd deg $n>1$, $\exists \theta \in K \setminus F$ and $\deg m_{\theta,F} = [F(\theta):F]$ is an odd integer ≥ 1. It has a root in F by (1), so ⨳. $\square$

Fact If F is formally real, then every odd degree extn of F is as well.

(Proof via Springer's Thm on quadratic forms.)

Cor If F is real closed, then any odd deg poly $f \in F[x]$ has a root in F. $\square$

Thm TFAE: (1) F is real closed.
(2) F is Euclidean and every odd-degree polynomial in $F[x]$ has a root in F
(3) $\sqrt{-1} \notin F$ and $K = F(\sqrt{-1})$ is algebraically closed.

Cor $\mathbb{R}$ is real closed and $\mathbb{C}$ is algebraically closed. $\square$

Pf of Thm (3) $\Rightarrow$ (1): F Euclidean so F formally real. Since the only proper alg extn of F is K (which is non real), F is real closed.

(1) $\Rightarrow$ (2): ✓

(2) $\Rightarrow$ (3): Have K quadratically closed. If $f(x) \in K[x]$ nonconstant then $f\bar{f} \in F[x]$. If $f\bar{f}$ has a root in K, then f does, so suffices

to show all $g \in F[x] - F$ have a root in K. Let E be the splitting field of $(x^2+1)g$ over F, which is a Galois extn

$$\begin{array}{ccc} E & & \\ | & & K \\ F & & \end{array}$$

Since F has no odd deg extns, get that $[E:F] = 2^n$. (If not a power of 2, fixed field of H = 2-Sylow subgp of $Gal(E/F)$ is odd degree.)

Since K has no ~~odd deg~~ quadratic extns (K quad closed b/c F Euclidean) get that $K = E$. Since E splits $(x^2+1)g(x)$, get that g has a root in K. $\square$

<u>Thm</u> [Artin-Schreier] Let C be any algebraically closed field, and $F \subsetneq C$ with $[C:F] < \infty$. Then $\text{char}(F) = 0$, F is real closed, and $C = F(\sqrt{-1})$.

<u>Pf</u> (Assuming char $F = 0$) <u>Claim</u> $[C:F]$ is a power of 2.

Assume for $\Rightarrow\Leftarrow$ that an odd prime $p \mid [C:F]$. Since C/F is finite Galois with $|Gal(C/F)| = [C:F]$ divisible by p, know $\exists H \leq Gal(C/F)$ of order p and $[C:\underbrace{C^H}_{=K}] = p$.

Fix $\zeta = \zeta_p \in C$. Since ζ has deg $\leq p-1$ over K, get $\zeta \in K$. Thus $C = K(x)$ where $x \in C$, $x^p = a \in K$.

Let $\langle\sigma\rangle = Gal(C/K) \cong C_p$ and take $y \in C$ s.t. $y^p = x$ (so $y^{p^2} = a$). Then $\sigma(y) = \alpha y$ for some α s.t. $\alpha^{p^2} = 1$.

If $\alpha^p = 1$, then $\sigma(x) = \sigma(y)^p = y^p = x$, $\Rightarrow\Leftarrow$, so α is a primitive p^2 root of unity. Thus $\sigma(\alpha) = \alpha^r$ for some r rel prime to p.

Whence $\sigma^2(y) = \alpha^{r+1} y$, $\sigma^3(y) = \alpha^{r^2+r+1} y$, etc., ultimately giving $y = \sigma^p(y) = \alpha^{r^{p-1}+\cdots+r+1} y$.

Thus $r^{p-1}+\cdots+r+1 \equiv 0 \pmod{p^2}$. Multiplying by r, get $r^p \equiv 1 \pmod{p^2}$. In particular, $r^p \equiv 1 \pmod{p}$, so (FLT) $r \equiv 1 \pmod{p}$, $r = 1+kp$ for some $k \in \mathbb{Z}$. But then

$$\begin{aligned}
r^{p-1}+\cdots+r+1 &= \frac{r^p-1}{r-1} \\
&= \frac{(1+kp)^p-1}{kp} \\
&= \frac{\binom{p}{1}kp+\binom{p}{2}(kp)^2+\binom{p}{3}(kp)^3+\cdots+(kp)^p}{kp} \\
&= p+\binom{p}{2}kp+\underbrace{\binom{p}{3}(kp)^2+\cdots+(kp)^{p-1}} \\
&\equiv p \pmod{p^2}
\end{aligned}$$

manifest for

and $\binom{p}{2}kp = p\frac{(p-1)}{2}kp = \frac{k(p-1)}{2}p^2$

is a multiple of p^2 since p odd.

This contradicts $r^p \equiv 1 \pmod{p^2}$.

Now know $[C:F]=2^n$ for some n. Claim $n=1$.

If $n \geq 2$, get $E \subseteq L \subseteq C$ with $[C:L]=[L:E]=2$ (by Galois thy + ~~Sylow~~ fact that gps of order p^n have subgps of order p^k $\forall\, 0 \leq k \leq n$). Get L Euclidean since C quad closed, so $\sqrt{-1} \notin L$. Then $E(\sqrt{-1})$ is another subfield of C with $[C:E(\sqrt{-1})]=2$, so $E(\sqrt{-1})$ Euclidean, ↯ b/c $\sqrt{-1} \in E(\sqrt{-1})$.

Therefore $[C:F]=2$. Again, $\sqrt{-1} \notin F$, so $F(\sqrt{-1})=C$. $\square$