Announcements

Midterm 3: tonight 7:00-8:30 Sidney Lu 1043

See policy email for details

HW10 will be posted today (due next Wed.)

Midterm 3 review

Integral domains, poly. rings, irreducibility

Basic tools: irreducibility, field ext'ns, degrees, splitting fields, min'l polys., tower law

Constructibility: 4 classical problems, type of ext'ns allowed

Separability: derivative criterion, irreds. over char 0 or fin. field

Galois theory:

- Compute automorphisms, fixed fields
- Characterization of Galois ext'n (autom. gp. size, poly. splitting)
- Galois correspondence (inc. properties e.g. normal subgps.)
- trace, norm, and sym. func. (lie in base field)

Important cases:

- finite fields
- cyclotomic ext'ns

Compute Galois gps.

- discriminant (def and A_n criterion)
- compute Gal. gp. for deg 2,3
- gens. and rel'ns and/or cycle type
  (find some automs. and determine the gp. they gen.)

Solvability by radicals:

- Solvable gps and solvability criterion (Galois' thm)
- Cardano's formula (don't need to memorize)
- Prove that a poly. is/isn't solvable by radicals

14.2.3) Determine the Galois gp of $f=(x^2-2)(x^2-3)(x^2-5)$
Determine all subfields of $Sp\, f$

$K := Sp_{\mathbb{Q}} f = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$

$[K:\mathbb{Q}] = 8$ by D&F #14.4.2 (on HW 7)

Since K is a splitting field $/\mathbb{Q}$, $K/\mathbb{Q}$ is Galois,
so $G := Gal(K/\mathbb{Q})$ has order 8

$$\left.\begin{array}{l} \sigma \in G \text{ must send } \sqrt{2} \mapsto \pm\sqrt{2} \\ \qquad\qquad\qquad\quad \sqrt{3} \mapsto \pm\sqrt{3} \\ \qquad\qquad\qquad\quad \sqrt{5} \mapsto \pm\sqrt{5} \end{array}\right\} \begin{array}{l} \text{8 possibilites, so} \\ \text{all must be valid} \\ \text{automorphisms} \end{array}$$

Let $\sigma_{ijk}: \begin{cases} \sqrt{2} \mapsto (-1)^i\sqrt{2} \\ \sqrt{3} \mapsto (-1)^j\sqrt{3} \\ \sqrt{5} \mapsto (-1)^k\sqrt{5} \end{cases}$ for $i,j,k \in \{0,1\}$

$\sigma_{ijk}\sigma_{abc} = \sigma_{i+a,\, j+b,\, k+c}$ taken mod 2

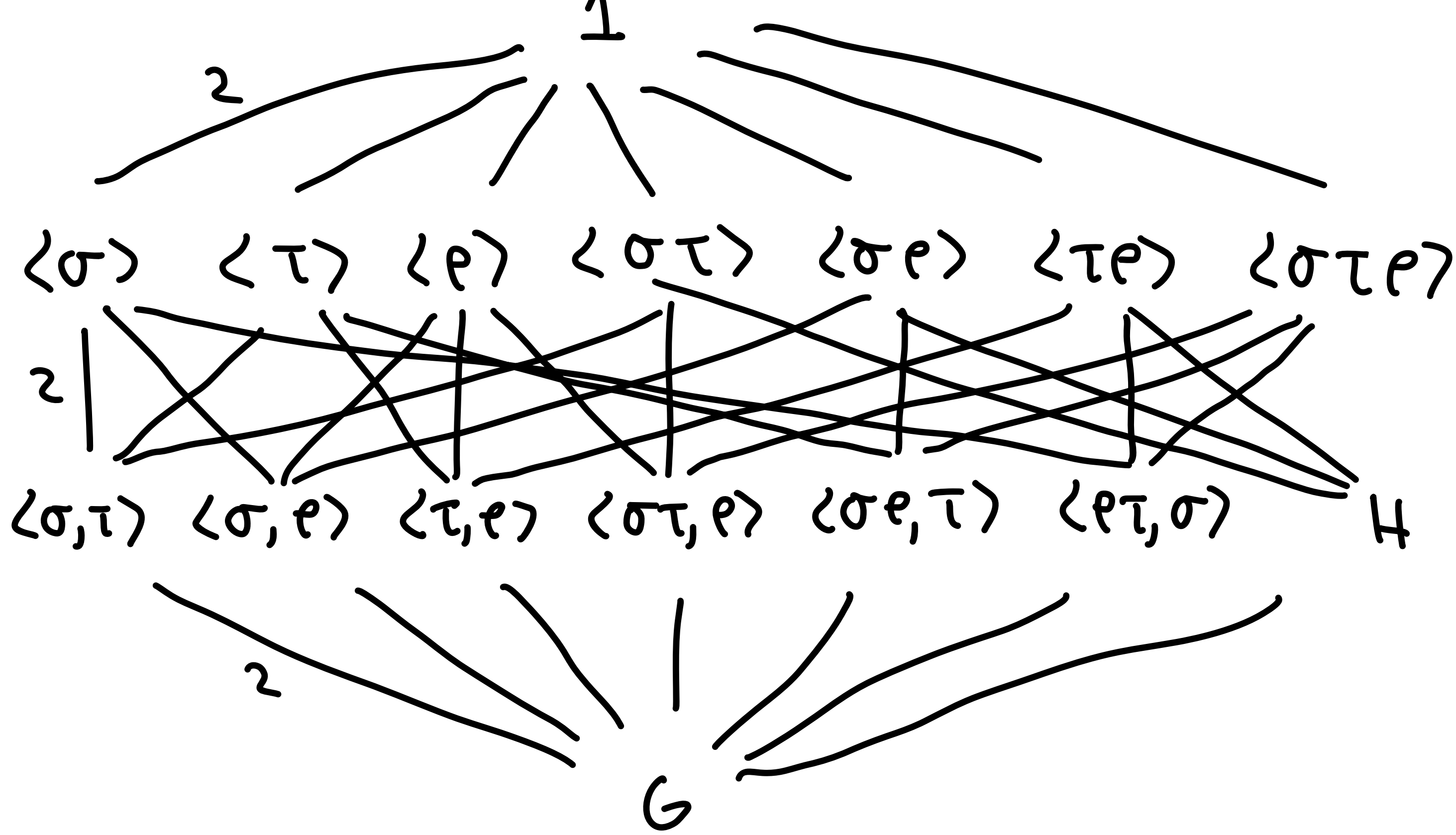
Let $\sigma := \sigma_{100}$, $\tau := \sigma_{010}$, $\rho := \sigma_{001}$

So $G = \{\sigma, \tau, \rho \mid \sigma^2 = \tau^2 = \rho^2 = 1,\ \sigma\tau = \tau\sigma,\ \sigma\rho = \rho\sigma,\ \tau\rho = \rho\tau\} \cong C_2 \times C_2 \times C_2$

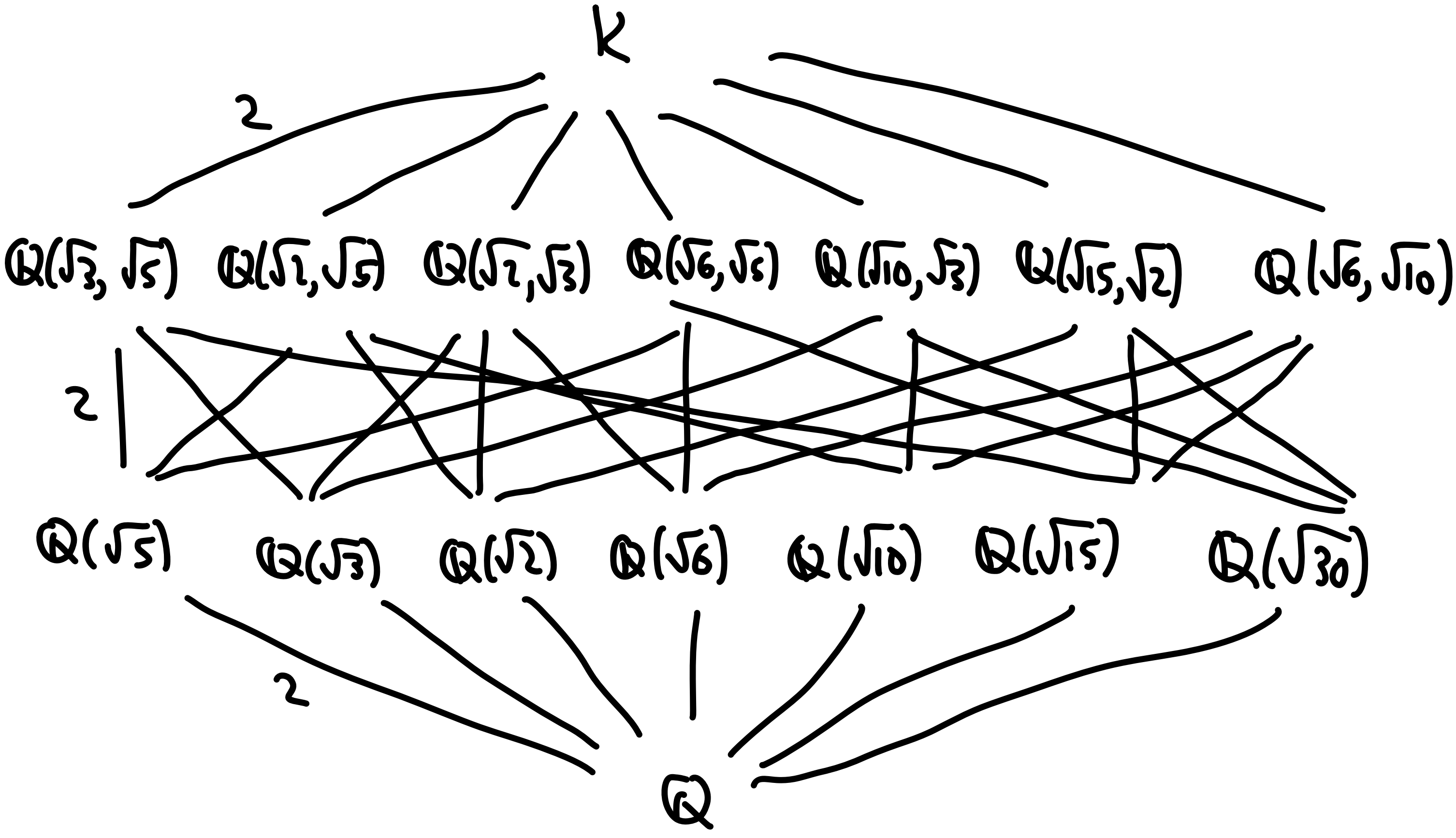
Subgps:

Order	Subgp.
1	$\{1\}$
2	$\langle \sigma \rangle \quad \forall \sigma \in G \setminus \{1\}$
4	$\{\sigma_{ijk} \mid i=0\} = \langle \tau, \rho \rangle$
	$\{\sigma_{ijk} \mid j=0\} = \langle \sigma, \rho \rangle$
	$\{\sigma_{ijk} \mid k=0\} = \langle \sigma, \tau \rangle$
	$\{\sigma_{ijk} \mid i=j\} = \langle \sigma\tau, \rho \rangle$
	$\{\sigma_{ijk} \mid i=k\} = \langle \sigma\rho, \tau \rangle$
	$\{\sigma_{ijk} \mid j=k\} = \langle \tau\rho, \sigma \rangle$
	$H := \{\sigma_{ijk} \mid i+j+k=0\} = \langle \sigma\tau, \sigma\rho, \tau\rho \rangle$
8	G

Subgp lattice



Int fields



14.4.4) Let $f(x) \in F[x]$ be an irred. poly. of deg n over F. Let $L = Sp_F f$, and let α be a root of f in L. If K is any Galois ext'n of F, show that

$$f(x) = \underbrace{p_1(x) \cdots p_m(x)}_{\substack{\text{irred. of} \\ \text{deg } d}} \in K[x]$$

where $d = [K(\alpha) : K] = [(L \cap K)(\alpha) : L \cap K]$ and

$m = n/d = [F(\alpha) \cap K : F]$

* Let's assume L/F is also Galois

Pf: Every factor of f lies in $L[x]$, so the irred. factorization of f in $K[x]$ equals the irred. factorization of f in $(K \cap L)[x]$, so the two def'ns of d are the same. We also have

$$n = [F(\alpha) : F] = \underbrace{[F(\alpha) : F(\alpha) \cap K]}_{d} \underbrace{[F(\alpha) \cap K : F]}_{m}, \text{ so}$$

the def of m is consistent too.

Let $H \leq Gal(L/F)$ correspond to the int field $L \cap K$. By our construction of min'l polys, for any root α of f in L,

$$m_{\alpha, L\cap K}(x) = \prod_{\beta \in H\alpha} (x-\beta)$$

Thus, the degs. of the irred. factors of $f(x)$ over $L \cap K$ equal the sizes of the H-orbits of $S := \{\text{roots of } f\}$

Since K/F is Galois, by prop. 4 of the Fun. Thm., $H \trianglelefteq G$. By Dummit & Foote Ex. 4.9a, since G acts transitively on S and H is normal, the H-orbits must be the same size.

(pf: transitivity $\Rightarrow S = \{g\alpha \mid g \in G\}$. Orbits are $Hg\alpha = gH\alpha$, which has order $|H\alpha|$)

Thus, all the p_i have the same degree, and this degree equals

$$\deg m_{\alpha, L\cap K}(x) = [(L\cap K)(\alpha) : L\cap K]$$

$\square$