MAT205 Assignment 2 — Solutions

Problem 1. The Splitting Field of $x^4 - 2$ over $\mathbb{Q}$

Let $f(x) = x^4 - 2$, let $\sqrt[4]{2}$ be the real positive fourth root of 2, and let $i = \sqrt{-1}$. Let E be the splitting field of f over $\mathbb{Q}$.

(a)

Solution. By Eisenstein's criterion at $p = 2$: 2 divides the lower coefficients $0, 0, 0, -2$ but not the leading 1, and $2^2 = 4 \nmid -2$. Hence $f = x^4 - 2$ is irreducible over $\mathbb{Q}$, so it is the minimal polynomial of $\sqrt[4]{2}$ and $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = \deg f = 4$.

(b)

Solution. Since $(i^k \sqrt[4]{2})^4 = i^{4k} \cdot 2 = 2$, the four distinct roots of f are $\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-\sqrt[4]{2}$, $-i\sqrt[4]{2}$. Their field is $\mathbb{Q}(\sqrt[4]{2}, i)$, because $i = (i\sqrt[4]{2})/\sqrt[4]{2}$ shows $i \in E$, and conversely all four roots lie in $\mathbb{Q}(\sqrt[4]{2}, i)$. So $E = \mathbb{Q}(\sqrt[4]{2}, i)$.

Now $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ while $i \notin \mathbb{R}$, so $i \notin \mathbb{Q}(\sqrt[4]{2})$; hence $x^2 + 1$ is irreducible over $\mathbb{Q}(\sqrt[4]{2})$ and $[E : \mathbb{Q}(\sqrt[4]{2})] = 2$. By the tower law,

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[4]{2})]\,[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

(c)

Solution. E is the splitting field of $x^4 - 2$, which is separable in characteristic 0; hence $E/\mathbb{Q}$ is a finite Galois extension and $|\operatorname{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = 8$.

(d)

Solution. Each of σ, τ permutes the roots of f and sends i to a root of $x^2 + 1$, so each extends to an automorphism of E fixing $\mathbb{Q}$.

Since $\sigma(i) = i$, $\sigma^k(\sqrt[4]{2}) = i^k \sqrt[4]{2}$; thus $\sigma^4 = \mathrm{id}$ and $\sigma^2(\sqrt[4]{2}) = -\sqrt[4]{2} \neq \sqrt[4]{2}$, so σ has order 4. Also $\tau^2 = \mathrm{id}$ and $\tau \neq \mathrm{id}$, so τ has order 2. Finally, using $\tau^{-1} = \tau$,

$$\tau\sigma\tau(\sqrt[4]{2}) = \tau\sigma(\sqrt[4]{2}) = \tau(i\sqrt[4]{2}) = -i\sqrt[4]{2} = \sigma^{-1}(\sqrt[4]{2}), \qquad \tau\sigma\tau(i) = \tau\sigma(-i) = \tau(-i) = i = \sigma^{-1}(i),$$

so $\tau\sigma\tau^{-1} = \sigma^{-1}$. Thus $\langle \sigma, \tau \rangle$ has the dihedral presentation $\langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1,\ \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$, i.e. $\langle \sigma, \tau \rangle \cong D_4$. As it has order $8 = |\operatorname{Gal}(E/\mathbb{Q})|$,

$$\operatorname{Gal}(E/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong D_4.$$

(e)

Solution. The eight elements are

$$1,\ \sigma,\ \sigma^2,\ \sigma^3,\ \tau,\ \sigma\tau,\ \sigma^2\tau,\ \sigma^3\tau.$$

Using $\sigma^4 = \tau^2 = 1$ and $\tau\sigma = \sigma^{-1}\tau = \sigma^3\tau$, so $\tau\sigma^k = \sigma^{-k}\tau$, the multiplication table (row $\cdot$ column) is

$\cdot$	1	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
1	1	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
σ	σ	σ^2	σ^3	1	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$	τ
σ^2	σ^2	σ^3	1	σ	$\sigma^2\tau$	$\sigma^3\tau$	τ	$\sigma\tau$
σ^3	σ^3	1	σ	σ^2	$\sigma^3\tau$	τ	$\sigma\tau$	$\sigma^2\tau$
τ	τ	$\sigma^3\tau$	$\sigma^2\tau$	$\sigma\tau$	1	σ^3	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^3\tau$	$\sigma^2\tau$	σ	1	σ^3	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	$\sigma^3\tau$	σ^2	σ	1	σ^3
$\sigma^3\tau$	$\sigma^3\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^3	σ^2	σ	1

Their orders: 1 has order 1; σ, σ^3 have order 4; and $\sigma^2, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau$ each have order 2. Since $\tau\sigma^2\tau^{-1} = (\tau\sigma\tau^{-1})^2 = \sigma^{-2} = \sigma^2$, the element σ^2 commutes with τ and with σ, hence with all of D_4; no other non-identity element is central. Therefore $Z(\operatorname{Gal}(E/\mathbb{Q})) = \langle \sigma^2 \rangle$.

(f)

Solution. The ten subgroups are:

- order 1: $\{1\}$;
- order 2: $\langle\sigma^2\rangle$ (the centre), $\langle\tau\rangle$, $\langle\sigma^2\tau\rangle$, $\langle\sigma\tau\rangle$, $\langle\sigma^3\tau\rangle$;
- order 4: $\langle\sigma\rangle$ (cyclic), $\langle\sigma^2,\tau\rangle = \{1,\sigma^2,\tau,\sigma^2\tau\}$, $\langle\sigma^2,\sigma\tau\rangle = \{1,\sigma^2,\sigma\tau,\sigma^3\tau\}$ (the last two are Klein four-groups);
- order 8: D_4.

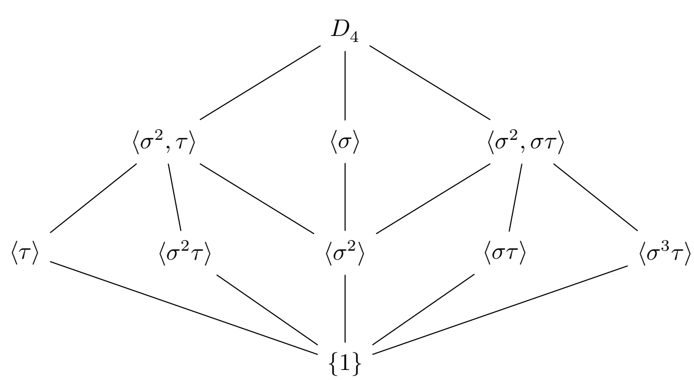
(g)

Solution. Write $\alpha = \sqrt[4]{2}$ (so $\alpha^2 = \sqrt{2}$). The actions on α and i are $\sigma : \alpha \mapsto i\alpha,\ i \mapsto i$ and $\tau : \alpha \mapsto \alpha,\ i \mapsto -i$, whence e.g. $\sigma^2 : \alpha \mapsto -\alpha$ (so σ^2 fixes $\sqrt{2}$ and i). Using $[E^H : \mathbb{Q}] = 8/|H|$ to fix the degree and exhibiting a generator fixed by H gives:

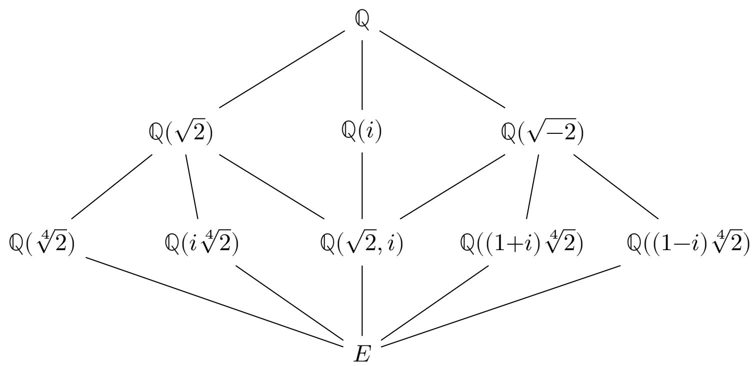
Subgroup H	order	fixed field E^H	$[E^H : \mathbb{Q}]$
$\{1\}$	1	$E = \mathbb{Q}(\sqrt[4]{2}, i)$	8
$\langle\tau\rangle$	2	$\mathbb{Q}(\sqrt[4]{2})$	4
$\langle\sigma^2\tau\rangle$	2	$\mathbb{Q}(i\sqrt[4]{2})$	4
$\langle\sigma\tau\rangle$	2	$\mathbb{Q}((1+i)\sqrt[4]{2})$	4
$\langle\sigma^3\tau\rangle$	2	$\mathbb{Q}((1-i)\sqrt[4]{2})$	4
$\langle\sigma^2\rangle$	2	$\mathbb{Q}(\sqrt{2}, i)$	4
$\langle\sigma\rangle$	4	$\mathbb{Q}(i)$	2
$\langle\sigma^2,\tau\rangle$	4	$\mathbb{Q}(\sqrt{2})$	2
$\langle\sigma^2,\sigma\tau\rangle$	4	$\mathbb{Q}(\sqrt{-2})$	2
D_4	8	$\mathbb{Q}$	1

Sample justifications. τ fixes $\alpha = \sqrt[4]{2}$, giving $\mathbb{Q}(\sqrt[4]{2})$; $\sigma^2\tau$ ($\alpha \mapsto -\alpha,\ i \mapsto -i$) fixes $i\alpha$, giving $\mathbb{Q}(i\sqrt[4]{2})$; $\sigma\tau$ fixes $(1+i)\alpha$, giving $\mathbb{Q}((1+i)\sqrt[4]{2})$, and $\sigma^3\tau$ fixes $(1-i)\alpha$. The centre $\langle\sigma^2\rangle$ fixes $\sqrt{2}$ and i, giving $\mathbb{Q}(\sqrt{2}, i)$. Among the order-4 subgroups, σ fixes i, $\langle\sigma^2,\tau\rangle$ fixes $\sqrt{2}$, and $\langle\sigma^2,\sigma\tau\rangle$ fixes $i\sqrt{2} = \sqrt{-2}$.

The two lattices (anti-isomorphic via $H \mapsto E^H$):



subgroups



intermediate fields (drawn upside-down)

(h)

Solution. The three order-4 subgroups have index 2, hence are normal; the centre $\langle\sigma^2\rangle$ is normal; and $\{1\}, D_4$ are normal. So the normal subgroups are

$$\{1\},\ \langle\sigma^2\rangle,\ \langle\sigma\rangle,\ \langle\sigma^2,\tau\rangle,\ \langle\sigma^2,\sigma\tau\rangle,\ D_4,$$

and the four non-central reflections $\langle\tau\rangle, \langle\sigma\tau\rangle, \langle\sigma^2\tau\rangle, \langle\sigma^3\tau\rangle$ are **not** normal. By the fundamental theorem, the intermediate fields normal over $\mathbb{Q}$ are exactly

$$E,\ \mathbb{Q}(\sqrt{2}, i),\ \mathbb{Q}(i),\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{-2}),\ \mathbb{Q},$$

while the four quartic fields are not. For instance $\mathbb{Q}(\sqrt[4]{2})$ contains the root $\sqrt[4]{2}$ of the irreducible $x^4 - 2$ but not the non-real root $i\sqrt[4]{2}$, so $x^4 - 2$ does not split there — not normal. Finally $\mathbb{Q}(\sqrt{2}, i)$ is biquadratic with $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(i)

Solution. Using $\tau\sigma^{-1}\tau = \sigma$,

$$[\sigma,\tau] = \sigma\tau\sigma^{-1}\tau^{-1} = \sigma(\tau\sigma^{-1}\tau) = \sigma\cdot\sigma = \sigma^2,$$

so $\sigma^2 \in [D_4, D_4]$. Since $D_4/\langle\sigma^2\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is abelian, $[D_4, D_4] \subseteq \langle\sigma^2\rangle$, hence $[D_4, D_4] = \langle\sigma^2\rangle$.

A subextension $\mathbb{Q} \subseteq F \subseteq E$ is Galois over $\mathbb{Q}$ with $\mathrm{Gal}(F/\mathbb{Q})$ abelian if and only if the corresponding subgroup $\mathrm{Gal}(E/F)$ contains $[D_4, D_4]$ (a subgroup containing the commutator subgroup is automatically normal, with abelian quotient). The largest such F corresponds to the smallest such subgroup, namely $[D_4, D_4] = \langle\sigma^2\rangle$. Therefore the largest such intermediate field is

$$K = E^{[D_4,D_4]} = E^{\langle\sigma^2\rangle} = \mathbb{Q}(\sqrt{2}, i), \qquad \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) \cong D_4/[D_4, D_4] \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Problem 2. Counting Irreducible Polynomials over Finite Fields

Throughout we use, as permitted, the structure of finite fields: $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois with $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle\mathrm{Fr}\rangle$ cyclic of order n (where $\mathrm{Fr}(\alpha) = \alpha^q$), and $\mathbb{F}_{q^n}$ has a unique subfield of size q^d for each $d \mid n$.

(a)

Solution. Let $m = [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$, so $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. The minimal polynomial g of α over $\mathbb{F}_q$ is irreducible of degree m and separable, and its roots are the conjugates of α, namely

$$\{\theta(\alpha) : \theta \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)\} = \{\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}\},$$

which are m distinct elements. This is exactly the $\langle \mathrm{Fr} \rangle$-orbit of α: the orbit closes up at the least m with $\alpha^{q^m} = \alpha$, i.e. with $\alpha \in \mathbb{F}_{q^m}$, i.e. $m = [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$. Hence the orbit has size m and equals the root set of g.

Conversely, every monic irreducible g of degree d over $\mathbb{F}_q$ is the minimal polynomial of each of its roots $\alpha \in \mathbb{F}_{q^d}$, whose orbit (of size d) is precisely the root set of g. Therefore monic irreducible polynomials of degree d over $\mathbb{F}_q$ correspond bijectively to $\langle \mathrm{Fr} \rangle$-orbits of size d.

(b)

Solution. By the subfield criterion, the subfields of $\mathbb{F}_{q^6}$ correspond to the divisors of 6 (namely $1, 2, 3, 6$), so they are

$$\mathbb{F}_q, \quad \mathbb{F}_{q^2}, \quad \mathbb{F}_{q^3}, \quad \mathbb{F}_{q^6}.$$

Inside $\mathbb{F}_{q^6}$ one has $\mathbb{F}_{q^a} \cap \mathbb{F}_{q^b} = \mathbb{F}_{q^{\gcd(a,b)}}$; in particular $\mathbb{F}_{q^2} \cap \mathbb{F}_{q^3} = \mathbb{F}_q$.

For $\alpha \in \mathbb{F}_{q^6}$, the field $\mathbb{F}_q(\alpha)$ is a subfield of $\mathbb{F}_{q^6}$, so $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] \in \{1, 2, 3, 6\}$; if $\alpha \notin \mathbb{F}_q$ the degree is 2, 3, or 6. By (a) the orbit size equals this degree, so the $\langle \mathrm{Fr} \rangle$-orbits inside $\mathbb{F}_{q^6} \setminus \mathbb{F}_q$ have exactly three possible sizes:

$$\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \text{ (size 2)}, \quad \alpha \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q \text{ (size 3)}, \quad \alpha \in \mathbb{F}_{q^6} \setminus (\mathbb{F}_{q^2} \cup \mathbb{F}_{q^3}) \text{ (size 6)}.$$

(Here $6 = 2 \cdot 3$ is the smallest degree that is neither prime nor a prime power, which is why three distinct orbit sizes appear.)

(c)

Solution. Counting elements of $\mathbb{F}_{q^6}$ by degree over $\mathbb{F}_q$:

- degree 1: $\mathbb{F}_q$, that is q elements;
- degree 2: $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, that is $q^2 - q$ elements;
- degree 3: $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$, that is $q^3 - q$ elements;
- degree 6: $\mathbb{F}_{q^6} \setminus (\mathbb{F}_{q^2} \cup \mathbb{F}_{q^3})$. By inclusion–exclusion $|\mathbb{F}_{q^2} \cup \mathbb{F}_{q^3}| = q^2 + q^3 - q$, so the degree-6 count is $q^6 - (q^3 + q^2 - q) = q^6 - q^3 - q^2 + q$.

These add up correctly: $q + (q^2 - q) + (q^3 - q) + (q^6 - q^3 - q^2 + q) = q^6$. By (a) the elements of degree d split into $\langle \mathrm{Fr} \rangle$-orbits of size d, each orbit corresponding to exactly one monic irreducible polynomial of degree d. Dividing each degree count by the orbit size gives

$$\text{degree } 2: \ \frac{q^2 - q}{2}, \qquad \text{degree } 3: \ \frac{q^3 - q}{3}, \qquad \text{degree } 6: \ \frac{q^6 - q^3 - q^2 + q}{6}.$$

(Each is an integer; for degree 6 this is the Gauss/Möbius count $\frac{1}{6} \sum_{d|6} \mu(d)\, q^{6/d} = \frac{1}{6}(q^6 - q^3 - q^2 + q)$.)