Math 404 HW 8 Solutions

Problem 8.1

Let ω be a primitive 7th root of unity. Show that $\mathbb{Q} \subset \mathbb{Q}(\omega)$ is a Galois extension and compute its Galois group.

Proof. Let $f(x) = x^7 - 1$. Then all the roots of f are of the form ω^i for some $1 \leq i \leq 7$, so $\mathbb{Q}(\omega)$ is the splitting field of f over $\mathbb{Q}$. Since $\mathbb{Q}$ is of characteristic zero, this extension is separable. Since splitting fields are normal, this extension is Galois.

I claim that the Galois group is $(\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$. To see this, let $p(x) = \frac{x^7-1}{x-1}$, and let $G = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$. We have previously shown that p is the irreducible polynomial for ω over $\mathbb{Q}$. Thus, we have that

$$|\mathbb{Q}(\omega) : \mathbb{Q}| = |G| = 6.$$

Any element $\sigma \in G$ is uniquely determined by where it sends ω, and it must send ω to some root of $p(x)$. That is, we must have $\sigma(\omega) = \omega^i$ for a unique $1 \leq i \leq 6$ (not $\omega^7 = 1$, as that is not a root of p). I claim that the function $\varphi : G \to (\mathbb{Z}/7\mathbb{Z})^\times$ defined by sending $\sigma \in G$ to the element $i \in (\mathbb{Z}/7\mathbb{Z})^\times$ so that $\sigma(\omega) = \omega^i$ yields a group isomorphism.

Injectivity of φ follows from the above discussion. Since

$$|G| = |(\mathbb{Z}/7\mathbb{Z})|^\times = 6,$$

we have that φ is bijective, so we just need to show that it is a homomorphism. To see this, let $\sigma_i, \sigma_j \in G$ be elements such that $\sigma_i(\omega) = \omega^i$ and similarly for σ_j. Write $ij = 7q + r$ with $1 \leq r \leq 6$ (the first inequality is satisfied because $i, j \in (\mathbb{Z}/7\mathbb{Z})^\times$) so that $r = ij$ in $\mathbb{Z}/7\mathbb{Z}$. We compute

We compute

$$\begin{aligned}\sigma_i \circ \sigma_j(\omega) &= \sigma_i(\omega^j) \\ &= (\sigma_i(\omega))^j \\ &= (\omega^i)^j \\ &= \omega^{ij} \\ &= \omega^{7q+r} \\ &= \omega^{7q}\omega^r \\ &= (\omega^7)^q\omega^r \\ &= 1^q\omega^r \\ &= \omega^r.\end{aligned}$$

This shows that

$$\varphi(\sigma_i \circ \sigma_j) = r = i \cdot j = \varphi(\sigma_i) \cdot \varphi(\sigma_j),$$

so φ is a homomorphism, as desired.

The final isomorphism $(\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$ comes from just noting that 3 generates $(\mathbb{Z}/7\mathbb{Z})^\times$, as do a couple other elements.

□

Problem 8.2

(a) Let $L = \mathbb{Q}(\sqrt{5}, i)$. Show that $L/\mathbb{Q}$ is Galois and compute its Galois group.

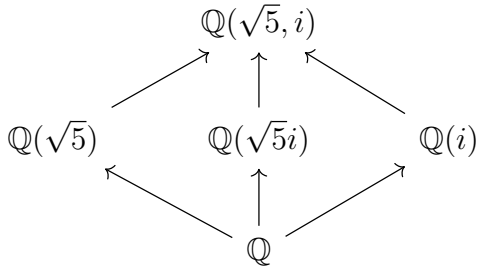
(b) Give the explicit correspondence between subgroups $H \subset \mathrm{Gal}(L/\mathbb{Q})$ and intermediate fields $\mathbb{Q} \subset E \subset L$.

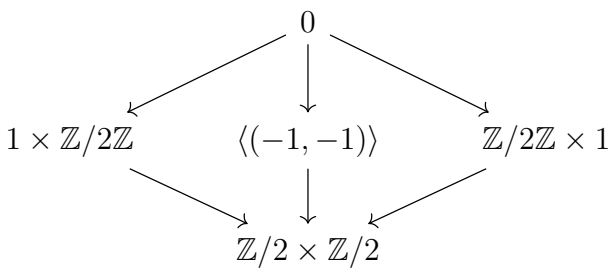
1. L is the splitting field of $(x^2 - 5)(x^2 + 1)$, so it is normal and finite. It is separable as we're in characteristic zero, so we're Galois. Let $G = \mathrm{Gal}(L/\mathbb{Q})$. Any element $\sigma \in G$ sends $\sqrt{5}$ to $\pm\sqrt{5}$, and sends $i \mapsto \pm i$. Thinking of $\mathbb{Z}/2\mathbb{Z}$ as the group on the symbols $\{+1, -1\}$ with multiplication, we get a map $\varphi : G \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sending σ to the "signs" of $\sigma(\sqrt{5})$ and $\sigma(i)$. Then we just check that it's an isomorphism, which is similar to the argument in problem 1.

□

2. We'll just give the two lattices of subgroups and intermediate fields, with arrows pointing from the smaller thing to the bigger thing. I also use the notation that if I have elements $g_1, \ldots, g_n$ in a group G, then I write $\langle g_1, \ldots, g_n \rangle$ to mean the subgroup of G generated by these elements.

   I made these diagrams using the following very heplful applet `https://tikzcd.yichuanshen.de/` which you can also find on github at `https://github.com/yishn/tikzcd-editor`.





Problem 8.3

Let L be the splitting field of $f(x) = x^3 - 2$ over $\mathbb{Q}$.

(a) Show that $L/\mathbb{Q}$ is Galois and compute its Galois group.

(b) Give the explicit correspondence between subgroups $H \subset \mathrm{Gal}(L/\mathbb{Q})$ and intermediate fields $\mathbb{Q} \subset E \subset L$.

(a) The action of the Galois group on the roots of f yields an embedding $\mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow S_3$, which turns out to be an isomorphism. The argument is exactly the same as the one for the splitting field of $x^3 - 5$ given at the end of class on May 19th.

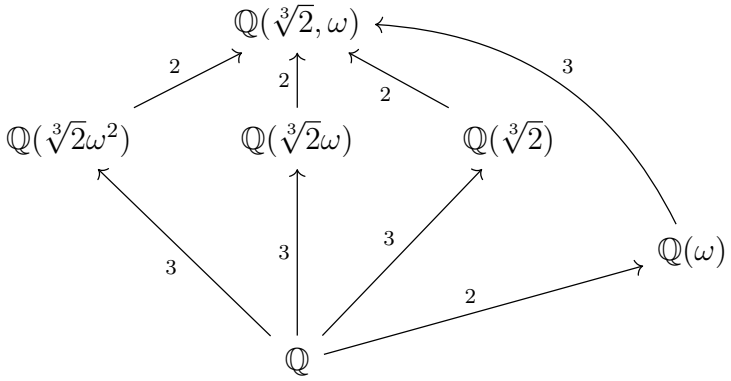
□

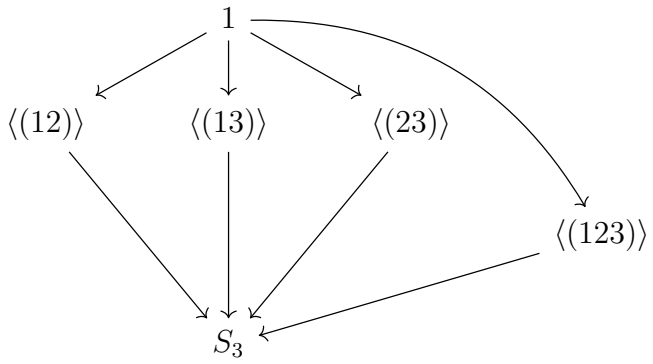
We give the correspondence on the next page.

(b) Let ω be a primitive 3rd root of unity. We number the roots of f as

(1) $\sqrt[3]{2}$
(2) $\sqrt[3]{2}\omega$
(3) $\sqrt[3]{2}\omega^2$.

With this labeling we build intermediate field and subgroup diagrams.





Problem 8.4

Let L be the splitting field of $f = x^4 - 2$ over $\mathbb{Q}$

(a) Show that $L/\mathbb{Q}$ is Galois and compute its Galois group.

(b) Give the explicit correspondence between subgroups $H \subset \mathrm{Gal}(L/\mathbb{Q})$ and intermediate fields $\mathbb{Q} \subset E \subset L$.

(a) First you can show $L = \mathbb{Q}(\sqrt[4]{2}, i)$ by at this point somewhat standard splitting field arguments. Since L is a splitting field over $\mathbb{Q}$, it is normal over $\mathbb{Q}$. Since $\mathbb{Q}$ has characteristic zero, any extension of $\mathbb{Q}$ is separable. So $L/\mathbb{Q}$ is finite, normal and separable, i.e. $L/\mathbb{Q}$ is Galois. We can show $|L : \mathbb{Q}| = 8$ by at this point familiar arguments, so we're looking for some group of order 8.

I claim that the Galois group is D_8, the dihedral group of order 8, with generators σ, τ defined by

$$\begin{aligned} \sigma(\sqrt[4]{2}) &= i\sqrt[4]{2} \\ \sigma(i) &= i \\ \tau(\sqrt[4]{2}) &= \sqrt[4]{2} \\ \tau(i) &= -i. \end{aligned}$$

To see this, note that $L/\mathbb{Q}(\sqrt[4]{2})$ is the splitting field of $x^2 + 1$, which is irreducible over $\mathbb{Q}(\sqrt[4]{2})$ (this field is contained in $\mathbb{R}$). So we get an automorphism τ of L fixing $\mathbb{Q}(\sqrt[4]{2})$ and sending $\tau(i) = -i$. This is the τ given above.

We also have that $L/\mathbb{Q}(i)$ is the splitting field of $x^4 - 2$. We can play a game of degrees of field extensions in towers to show that $|L : \mathbb{Q}(i)| = 4$. Since $L = \mathbb{Q}(i)(\sqrt[4]{2})$ and $\sqrt[4]{2}$ is a root of $x^4 - 2$, we must have that $x^4 - 2$ is irreducible over $\mathbb{Q}(i)$. Thus, we get an automorphism σ of L fixing $\mathbb{Q}(i)$ and sending $\sqrt[4]{2}$ to $i\sqrt[4]{2}$, as $i\sqrt[4]{2}$ is another root of the minimal polynomial for $\sqrt[4]{2}$ over $\mathbb{Q}(i)$.

We may directly compute that σ is of order 4. So $\langle \sigma, \tau \rangle \subset \mathrm{Gal}(L/\mathbb{Q})$ is a subgroup of order larger than 4. Since $\mathrm{Gal}(L/\mathbb{Q})$ has order 8,

Lagrange's theorem yields $\mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle$. So we have generators, what are the relations?

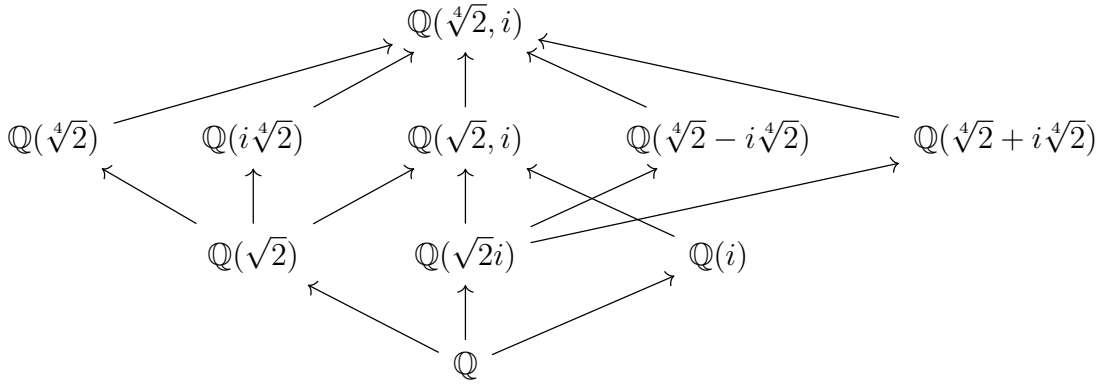
By looking at the action on $\sqrt[4]{2}$ and i, we may compute

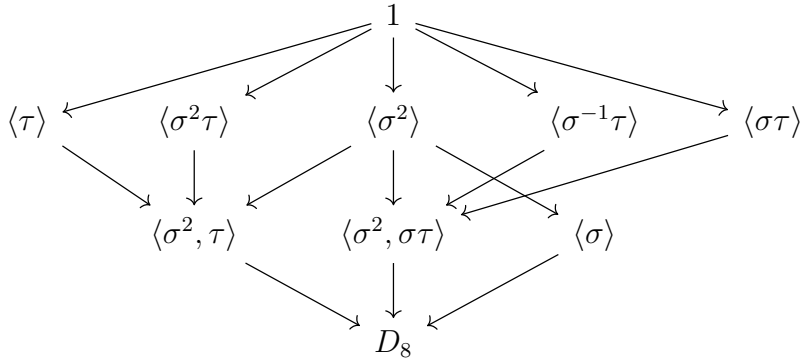
$$\sigma^4 = \tau^2 = \mathrm{id}, \text{ and } \tau\sigma\tau = \sigma^3 = \sigma^{-1}.$$

These are the defining relations for the Dihedral group D_8 (with σ as rotation by $\pi/2$ and τ a reflection). So we get a homomorphism $\varphi : D_8 \to \mathrm{Gal}(L/\mathbb{Q})$. We know that φ is surjective because we already showed that σ and τ generate $\mathrm{Gal}(L/\mathbb{Q})$. Since both groups are finite of the same order, we must have that φ is an isomorphism, as desired.

□

(b) First, we just give the correspondence (every arrow indicating a field extension is degree 2, so I didn't label them to avoid cluttering the diagram)





Here are some hints for how you might go about getting the above diagrams. On the intermediate fields side, I think every field pictured besides the fields $\mathbb{Q}(\sqrt[4]{2} \pm i\sqrt[4]{2})$ is a natural one to consider. Then you can just test and see which elements of D_8 fix these fields by seeing which ones fix the elements generating them. You have a check for this because if an intermediate field $\mathbb{Q} \subset E \subset L$ corresponds to a subgroup $H \subset D_8$, you know that $|L : E| = |H|$.

Then you just have two subgroups of D_8 missing, and you have to figure out their fixed fields.

Finding elements fixed by a given subgroup

Homework 2 problem 4

One way to do this is to use a result almost completely analogous to problem 4 on homework 2, and hinted at in class. That is, say you have a subgroup $H \subset \mathrm{Gal}(L/\mathbb{Q})$, and an element $\lambda \in L$. Let $\{\lambda_1, \ldots, \lambda_n\}$ be the orbit of λ under the action of H. Let $s \in \mathbb{Q}[x_1, \ldots, x_n]$ be a symmetric polynomial (that is, it's fixed by the S_n action on $\mathbb{Q}[x_1, \ldots, x_n]$ given by permuting the variables). Then $s(\lambda_1, \ldots, \lambda_n)$ is fixed by H. Prove this yourself, you'll see the same proof as in the homework problem goes through. Good choices of λ and s then can have a hope to yield generators for L^H, the fixed field of H.

For instance, since $(\sigma\tau)^2 = \mathrm{id}$, the orbit of $\sqrt[4]{2}$ under the action of $\langle \sigma\tau \rangle$ is just

$$\{\sqrt[4]{2}, \sigma\tau(\sqrt[4]{2})\} = \{\sqrt[4]{2}, i\sqrt[4]{2}\}.$$

so any symmetric polynomial in 2 variables, evaluated at these two elements, will yield an element fixed by $\langle \sigma\tau \rangle$. Natural choices for symmetric polynomials are the two elementary symmetric polynomials, which yield the elements $\sqrt[4]{2} + i\sqrt[4]{2}$ and $\sqrt[4]{2}(i\sqrt[4]{2}) = i\sqrt{2}$. These two elements generate the two intermediate fields which are fixed by $\sigma\tau$, one containing the other.

Computing with a basis

Another way you can figure out which field elements are fixed by a given element of the Galois group is to compute with a basis well-tailored to the action of the Galois group.

For instance, the proof of the multiplicative property of the degree yields that $L/\mathbb{Q}$ has a basis

$$B = \{1, \sqrt[4]{2}, (\sqrt[4]{2})^2 = \sqrt{2}, (\sqrt[4]{2})^3, i\sqrt[4]{2}, i\sqrt{2}, i(\sqrt[4]{2})^3\}.$$

So you can just directly compute what an element of the Galois group does to a given linear combination of these basis elements, and then the field felements fixed by the group element are those which are the same linear combination before and after the action of the group element.

For example, let $A, B, C, \ldots, H \in \mathbb{Q}$, and compute

$$\sigma^2\tau\Big(A + B\sqrt[4]{2} + C\sqrt{2} + D(\sqrt[4]{2})^3 + Ei + Fi\sqrt[4]{2} + Gi\sqrt{2} + Hi(\sqrt[4]{2})^3\Big) =$$
$$A - B\sqrt[4]{2} + C\sqrt{2} - D(\sqrt[4]{2})^3 - Ei + Fi\sqrt[4]{2} - Gi\sqrt{2} + Hi(\sqrt[4]{2})^3.$$

Thus, the elements of $L^{\langle\sigma^2\tau\rangle}$ are those with $B = D = E = G = 0$. Thus, $L^{\langle\sigma^2\tau\rangle}$ has basis

$$\{1, \sqrt{2}, i\sqrt[4]{2}, i(\sqrt[4]{2})^3\} = \{1, -(i\sqrt[4]{2})^2, i\sqrt[4]{2}, -(i\sqrt[4]{2})^3\}.$$

Since $i\sqrt[4]{2}$ has minimal polynomial $x^4 - 2$, this latter form for a basis of $L^{\langle\sigma^2\tau\rangle}$ yields

$$L^{\langle\sigma^2\tau\rangle} = \mathbb{Q}(i\sqrt[4]{2}).$$

□

Problem 8.5

Let K be a field with $\mathrm{Char}(K) \neq 3$. Suppose that $f(x) = x^3 - 3x + 1 \in K[x]$ is irreducible. Let $L = K(\alpha)$ where α is a root of f. Prove that f splits over L, and deduce that $K \subseteq L$ is a Galois extension with Galois group $\mathbb{Z}/3\mathbb{Z}$.

Proof. Polynomial long division yields

$$f(x) = (x - \alpha)(x^2 + \alpha x + \alpha^2 - 3).$$

Let us for the moment assume $\mathrm{Char}(K) \neq 2$, as well. Then the quadratic formula applies, and we can compute the roots of $f/(x - \alpha)$ as

$$\begin{aligned} x &= \frac{-\alpha \pm \sqrt{12 - 3\alpha^2}}{2} \\ &= \frac{-\alpha \pm (-4 + \alpha + 2\alpha^2)}{2} && \text{(by the hint)} \\ &= \{-2 - \alpha - \alpha^2, -2 + \alpha^2\}. \end{aligned}$$

This last form for the roots also makes sense in characteristic 2, and indeed you can plug these elements into $f/(x-\alpha)$ in characteristic 2 and verify that you still get zero. These roots also clearly live in $L = K(\alpha)$, so we have that f splits in $K(\alpha)$

Thus, we have that L is the splitting field of f, and in particular it is normal over K. Since $f' = 3x^2 - 3 \neq 0$ and f is irreducible, we have that f is separable, so these three roots are distinct. We can show that $K \subset L$ is Galois in at least two ways. One is to cite a hard theorem that if $L = K(\alpha_1, \ldots, \alpha_n)$ with each α_i separable over K, then L is separable over K, which is proven at `https://stacks.math.columbia.edu/tag/09GZ` (it's lemma 9.12.10, but you need the stuff before it to make sense of it).

Another starts by noting that $L \cong K[x]/f$. Since f is separable, there are three distinct roots of f in L. Sending x to each of these three roots yields three distinct automorphisms of L, fixing K. Thus, $|\operatorname{Gal}(L/K)| \geq 3$. But we also have $|\operatorname{Gal}(L/K)| \leq |L : K|$ for any finite extension. Since $|L : K| = 3$, we must have equality in the above inequalities, and the extension is Galois.

The final result follows from the fact that any group of order 3 is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ (indeed any group of prime order p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$).

□