Homework 10 (Due April 28, 2025)

Jack Hyatt

MATH 547 - Algebraic Structures II - Spring 2025

June 8, 2025

Justify all of your answers completely.

1. Let f_n denote the nth cyclotomic polynomial. Let $E = \mathbb{Q}(z_1)$ be the splitting field of f_n over $\mathbb{Q}$, where $z_1 = e^{\frac{2\pi}{n}}$ and let $G = Gal(E/\mathbb{Q})$.
   We say in class that $G = \{\sigma_k : 1 \le k \le n, \gcd(k,n) = 1\}$, where σ_k is the unique $\mathbb{Q}$-automorphism of E with $\sigma_k(z_1) = (z_1)^k$.
   Let $\phi : \mathbb{Z}_n^* \to G$ be defined as $\phi([k]_n) = \sigma_k$.

   (a) Verify that ϕ is a well-defined functioned.

   Let $k \equiv \ell \mod n$. Then $xn + \ell = k$ and

   $$z_1^k = (e^{2i\pi/n})^k = (e^{2i\pi/n})^{xn+\ell} = (e^{2i\pi/n})^{xn+\ell} = (e^{2i\pi/n})^\ell = z_1^\ell$$

   So then $\sigma_k(z_1) = \sigma_\ell(z_1)$. Since z_1 generates E over $\mathbb{Q}$, and automorphisms are defined by their mappings of the generators, it implies that $\sigma_k = \sigma_\ell$.

   (b) Verify that ϕ is a group homomorphism.

   $$\phi([k]_n \cdot [\ell]_n) = \phi([k\ell]_n) = \sigma_{k\ell}$$
   $$\phi([k]_n)\phi([\ell]_n) = \sigma_k\sigma_\ell = \sigma_{k\ell}$$

   (c) Verify that ϕ is one to one.

   Let $\phi([k]_n) = \phi([\ell]_n)$. Then $\sigma_k = \sigma_\ell$, which gives $z_1^k = z_1^\ell \implies e^{2ik\pi/n} = e^{2i\ell\pi/n}$. So

   $$2i\pi\frac{k}{n} = 2i\pi\left(\frac{\ell}{n} + x\right) \implies k = \ell + nx \implies k \equiv \ell \mod n$$

2. Let E denote the splitting field of $f(x) = x^3 - 2$ over $\mathbb{Q}$. Recall that $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where ω is a primitive 3rd root of 1, and that $[E : \mathbb{Q}] = 6$. Let $G = \mathrm{Gal}(E/\mathbb{Q})$.

   (a) Prove that G is isomorphic to S_3 (you may use the facts that were stated in class).

Proof. Since $[E:\mathbb{Q}] = 6$, then $|G| = 6$. We know that G is isomorphic to a subgroup to S_3, since it is the Galois group of the splitting field of degree 3. The only subgroup of S_3 with order 6 is S_3 itself. So G is isomorphic to S_3. ∎

(b) Find an element of G that has order equal to 3. Describe this element by saying what it does to the two generators of E over $\mathbb{Q}$, and verify that it has order 3.

Proof. Consider the automorphism defined by, $\sigma(\sqrt[3]{2}) = \sqrt[3]{4}$ and $\sigma(\omega) = \omega$. Clearly, it is an element of $\mathrm{Gal}(E/\mathbb{Q})$. Now to check that the order is not 2, which would make the order 3 since G is isomorphic to S_3 and that has elements of max degree 3.

$$\begin{aligned}\sigma^2(\sqrt[3]{2}) &= \sigma(\sqrt[3]{4}) \\ &= \sigma((\sqrt[3]{2})^2) \\ &= (\sigma(\sqrt[3]{2}))^2 \\ &= (\sqrt[3]{4})^2 \\ &= 2\sqrt[3]{2} \neq \sqrt[3]{2}\end{aligned}$$

Since $\sigma^2(\sqrt[3]{2}) \neq \sqrt[3]{2}$, we can immediately say the order is not 2. ∎

3. Using the notation from problem 2., let H denote the subgroup of G generated by the element you found in part 2b.
Find the fixed field of H, $E^H = \{x \in E : \sigma(x) = x \ \forall \sigma \in H\}$. Give your answer in the form $E = \mathbb{Q}(\dots)$ (specify what elements are adjoined to $\mathbb{Q}$ in order to get E). Prove your answer.
(hint: use a basis for E over $\mathbb{Q}$ to express a general element of E as a linear combination of the basis elements. Solve for the coefficients in the linear combination that ensure $\sigma(x) = x$ for $\sigma \in H$).

Proof. Let $H = \{id, \sigma, \sigma^2\}$. Let's express σ with how it sends an arbitrary element.

$$\sigma(a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\omega + e\sqrt[3]{2}\omega + f\sqrt[3]{4}\omega) = a + b\sqrt[3]{4} + 2c\sqrt[3]{2} + d\omega + e\sqrt[3]{4}\omega + 2f\sqrt[3]{2}\omega$$

We then end up with the equations:

$$\begin{aligned} a &= a & b &= 2c & e &= 2f \\ d &= d & c &= b & f &= e \end{aligned}$$

So then we have $b = c = e = f = 0$. So $E^H = \{a + d\omega : a, d \in \mathbb{Q}\}$, which clearly equals $\mathbb{Q}(\omega)$. ∎

4. The splitting field of $x^4 + 1$ over $\mathbb{Q}$ is $E = \mathbb{Q}(\sqrt{2}, i)$ (you don't need to prove this) and its Galois group G is isomorphic to the Klein 4-group $\mathbb{Z}_2 \times \mathbb{Z}_2$ (you don't need to prove this either).

(a) How many distinct fields L are there such that $\mathbb{Q} \subseteq L \subseteq E$? Justify your answer.

Proof. By the Fundamental Theorem of Galois Theory, we can just count the number of subgroups of G to find our answer, or subsequently subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$. Every non-identity element (3 of them) of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has degree 2, which means they generate a cyclic subgroup of order 2. So there are 3 subgroups of order 2. Including the entire group and the trivial identity subgroup, there are 5 subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$. So there are 5 non-isomorphic intermediary fields. ■

(b) Consider $L = \mathbb{Q}(\sqrt{2}i)$. Write out all the elements of $\mathrm{Gal}(E/L)$ by starting with the 4 elements of G and seeing which ones fix L.

Proof. Let us denote elements of G by how they map the generators with tuples (abusing notation ☺).

$$G = \{id, \sigma((\sqrt{2}, i)) = (-\sqrt{2}, i)\}, \tau((\sqrt{2}, i)) = (\sqrt{2}, -i), \gamma((\sqrt{2}, i)) = (-\sqrt{2}, -i)\}$$

Since L is an intermediary extension between $\mathbb{Q}$ and E, we only need to check the elements of G for automorphisms that fix L.
We only need to check the generators, as the automorphisms are homomorphisms. Clearly id fixes $\sqrt{2}i$.

$$\sigma(\sqrt{2}i) = \sigma(\sqrt{2})\sigma(i) = -\sqrt{2}i \neq \sqrt{2}i$$

$$\tau(\sqrt{2}i) = \tau(\sqrt{2})\tau(i) = \sqrt{2}(-i) \neq \sqrt{2}i$$

$$\gamma(\sqrt{2}i) = \gamma(\sqrt{2})\gamma(i) = -\sqrt{2}(-i) = \sqrt{2}i$$

So the only elements of $\mathrm{Gal}(E/L)$ are id and γ. ■