Homework #8

Due **Wednesday, April 1** in Gradescope by **11:59 pm ET**

READ Sections 6.1, 6.2, 6.3 in Cox

WATCH 1. Video 19: Another Proof of Galois Degree (15:46)
2. Video 20: Galois as Permutations (11:30)
3. Video 21: Semidirect Products (15:21)

WRITE AND SUBMIT solutions to the following problems.

Problem 1. (12 points) Cox, Section 6.1, Exercise 2, variant:
Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, let $K_2 = \mathbb{Q}(\sqrt{2})/\mathbb{Q}$, and let $K_3 = \mathbb{Q}(\sqrt{3})/\mathbb{Q}$, so that $L/K_i/\mathbb{Q}$ for $i = 1, 2$.

(a) Apply Proposition 5.1.8 to L/K_3 to show that there is some $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{3}) = \sqrt{3}$.

(b) Apply Proposition 5.1.8 to L/K_2 to show that there is some $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\tau(\sqrt{2}) = \sqrt{2}$ and $\tau(\sqrt{3}) = -\sqrt{3}$.

(c) Combine parts (a) and (b) with Example 6.1.10 to prove that $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Problem 2. (20 points) Cox, Section 6.1, Exercises 5–6, variant:
Let $m_1, \ldots, m_n \in \mathbb{Z}$ be pairwise relatively prime squarefree integers, none of which is 1. [That is, no m_i is 1 or is divisible by the square of any prime, and for all $i \neq j$, we have $\gcd(m_i, m_j) = 1$.]

(a) Prove that $\sqrt{m_n} \notin \mathbb{Q}\big(\sqrt{m_1}, \ldots, \sqrt{m_{n-1}}\big)$. [**Suggestion**: Induction on n.]

(b) Use Theorem 6.2.1 to prove that $\mathrm{Gal}\left(\mathbb{Q}\big(\sqrt{m_1}, \ldots, \sqrt{m_n}\big)/\mathbb{Q}\right)$ has order 2^n.

(c) Prove that $\left|\,\mathrm{Gal}\left(\mathbb{Q}\big(\sqrt{6}, \sqrt{10}, \sqrt{15}\big)/\mathbb{Q}\right)\right| \leq 4$.

[**Note**: For part (b), using the ideas of Problem 1, can you prove that
$\mathrm{Gal}\left(\mathbb{Q}\big(\sqrt{m_1}, \ldots, \sqrt{m_n}\big)/\mathbb{Q}\right) \cong (\mathbb{Z}/2\mathbb{Z})^n$? Here, of course, G^n denotes $G \times \cdots \times G$.
And can you prove that the Galois group in part (c) is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$?]

Problem 3. (8 points) Cox, Section 6.2, Exercise 3:
Let $L = \mathbb{Q}(\zeta_5, \sqrt[5]{2})$. Recall that the minimal polynomial of ζ_5 over $\mathbb{Q}$ is $\Phi_5 = x^4 + x^3 + x^2 + x + 1$.

(a) Prove that $[L : \mathbb{Q}] = 20$.

(b) Prove that L is the splitting field of $x^5 - 2$ over $\mathbb{Q}$, and conclude (by Theorem 6.2.1) that $|\,\mathrm{Gal}(L/\mathbb{Q})| = 20$.

Problem 4. (16 points) Cox, Section 6.2, Exercise 5:
Let $\mathrm{char}\, F = p$, and suppose $f = x^p - x + a \in F[x]$ is irreducible over F. Let $L = F(\alpha)$, where α is a root of f; in Exercise 5.3.16 (Homework 7, Problem 6), you showed that L/F is normal and separable.

(a) Prove $|\,\mathrm{Gal}(L/F)| = p$. [Of course, it follows that $\mathrm{Gal}(L/F) \cong \mathbb{Z}/p\mathbb{Z}$, by Lagrange.]

(b) Recall from Exercise 5.3.16 that $\alpha + 1$ is a root of f. For each $i = 0, \ldots, p-1$, prove that there is a unique element of $\mathrm{Gal}(L/F)$ that takes α to $\alpha + i$.

(c) Find an explicit isomorphism $\mathrm{Gal}(L/F) \cong \mathbb{Z}/p\mathbb{Z}$. [And justify your claims, of course.]

(continued next page)

Problem 5. (5 points) Cox, Section 6.2, Exercise 6: Let $f \in F[x]$ be irreducible and separable of degree $n \geq 1$, and let L/F be the splitting field of f over F. Prove that n divides $|\operatorname{Gal}(L/F)|$.

Problem 6. (18 points) Cox, Section 6.3, Exercise 2, variant:
For each of the following Galois groups, find an explicit subgroup of S_4 that it is isomorphic to, in that it permutes the roots of the given quartic polynomial according to that subgroup of S_4. [Of course, justify your answers.]

(a) (6 points) $\operatorname{Gal}(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q})$, with $\mathbb{Q}(i,\sqrt{2})$ as the splitting field of $f = x^4 - 4$ over $\mathbb{Q}$.

(b) (12 points) $\operatorname{Gal}(\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q})$, with $\mathbb{Q}(i,\sqrt[4]{2})$ as the splitting field of $g = x^4 - 2$ over $\mathbb{Q}$.

Problem 7. (10 points) Cox, Section 6.3, Exercise 4:
Let $\alpha = \sqrt{2+\sqrt{2}}$, and let $L = \mathbb{Q}(\alpha)$. In Exercise 5.1.6 (Homework 5, Problem 7), you showed that $f = x^4 - 4x^2 - 2$ is the minimal polynomial of α over $\mathbb{Q}$, with splitting field L. Prove that $\operatorname{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.

Problem 8. (15 points) Cox, Section 6.4, Exercise 7:
Prove that S_n is generated by the transposition $\tau = (1\ 2)$ and the n-cycle $\sigma = (1\ 2\ \ldots\ n)$
[**Note**: It's a standard fact from Math 350 that the transpositions generate S_n. So I'd suggest you prove that every transposition $(i\ j)$ can be expressed in terms of τ and σ.]

Optional Challenges (do NOT hand in): Cox Problems 6.2 #4, 6.3 #6,7

Questions? You can ask in:

Class: MWF 9:00am – 9:50am, SCCE C101

My office hours: in my office (SMUD 406):
Mon 2:00–3:30pm
Tue 1:30–3:15pm
Fri 1:00–2:00pm

Also, you may email me any time at `rlbenedetto@amherst.edu`