Math 418, Spring 2024 – Homework 8

Due: Wednesday, April 10th, at 9:00am via Gradescope.

Instructions: Students should complete and submit all problems. Textbook problems are from Dummit and Foote, *Abstract Algebra, 3rd Edition.* All assertions require proof, unless otherwise stated. Typesetting your homework using LaTeX is recommended, and will gain you 2 bonus points per assignment.

1. **Dummit and Foote #14.2.6:** *Let $K = \mathbb{Q}(\sqrt[8]{2}, i)$ and let $F_1 = \mathbb{Q}(i), F_2 = \mathbb{Q}(\sqrt{2}), F_3 = \mathbb{Q}(\sqrt{-2})$. Prove that $Gal(K/F_1) = \mathbb{Z}/8\mathbb{Z}$, $Gal(K/F_2) = D_8$, $Gal(K/F_3) = Q_8$. (Hint: use the example in Section 14.2, and the diagrams on pages 580-1)*

   Solution. Use the example in Section 14.2, and the diagrams on pages 580-1. These diagrams (along with the Galois correspondence) tell us that $\mathrm{Gal}(K/F_1) = \langle\sigma\rangle, \mathrm{Gal}(K/F_2) = \langle\sigma^2, \tau\rangle, \mathrm{Gal}(K/F_3) = \langle\sigma^2, \tau\sigma^3\rangle$. σ has order 8, so $\mathrm{Gal}(K/F_1) = \mathbb{Z}/8\mathbb{Z}$.

   The dihedral group of order 8 has the presentation $\langle s, t | s^4 = t^2 = 1, tst = s^{-1}\rangle$. We have $(\sigma^2)^4 = 1, \tau^2 = 1$, and $\tau\sigma^2\tau = \tau^2(\sigma^3)^2 = (\sigma^2)^{-1}$, so since $\mathrm{Gal}(K/F_2)$ has order 8, it must be D_8.

   Finally, the quaternion group has the presentation $\langle n, i, j, k | n^2 = 1, i^2 = j^2 = k^2 = ijk = n\rangle$. Let $n = \sigma^4, i = \sigma^2, j = \sigma\tau = \tau\sigma^3, k = \tau\sigma = \sigma^3\tau$. Then all the relations of Q_8 are satisfied (for example, $ijk = \sigma^2\sigma\tau\tau\sigma = \sigma^4 = n$), so since $\mathrm{Gal}(K/F_3)$ has order 8, it must be Q_8.

   (There are simpler ways to do this if we assume knowledge about finite groups of order 8. In particular, D_8 and Q_8 are the only nonabelian groups of order 8, and we can distinguish between them by comparing the number of elements of order 2.)

2. **Dummit and Foote #14.2.7:** *Determine all the subfields of the splitting field of $x^8 - 2$ which are Galois over $\mathbb{Q}$. (Hint: use the example in Section 14.2, and the diagrams on pages 580-1)*

   Solution. Use the example in Section 14.2, and the diagrams on pages 580-1. Let K be the splitting field of $x^8 - 2$. By the Fundamental Theorem of Galois theory, $E \subset K$ is Galois over the base field $\mathbb{Q}$ if and only if $\mathrm{Aut}(K/E)$ (the corresponding group to E in the diagrams) is normal in $G = \mathrm{Gal}(K/\mathbb{Q})$. This is a group-by-group check. Use the relation $\sigma\tau\sigma^{-1} = \tau\sigma^2$, and the fact that any index-2 subgroup is normal; conjugate the generators by both σ and τ to see if their images generate the same group. To be conjugate, subgroups must have the same number of generators, which must have the same orders.

We conclude that the normal subgroups in G are $G, \langle\sigma^2,\tau\rangle, \langle\sigma\rangle, \langle\sigma^2,\tau\sigma^3\rangle, \langle\sigma^2\rangle, \langle\sigma^4\rangle$, and 1, and therefore the intermediate fields which are Galois over $\mathbb{Q}$ are $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(i,\sqrt{2}), \mathbb{Q}(i,\sqrt[4]{2})$, and $K = \mathbb{Q}(i,\sqrt[8]{2})$.

3. **Dummit and Foote #14.2.14:** *Show that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a cyclic quartic field, i.e., is a Galois extension of degree 4 with cyclic Galois group.*

   Solution. Let $f(x) = x^4 - 4x^2 + 2$. This is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with the prime 2, and its roots (over a splitting field) are $\pm\theta_\pm := \pm\sqrt{2\pm\sqrt{2}}$ (note: distinct). Since $\theta_+\theta_- = \sqrt{2}$, $\theta_- = \frac{\theta_+^2-2}{\theta_+} \in \mathbb{Q}(\theta_+)$, so $\mathbb{Q}(\theta_+)$ is the splitting field for f, and therefore is Galois over $\mathbb{Q}$.

   Since the degree of the extension is 4, to show that the Galois group is cyclic, we just need to show that is has an element of degree 4. One such possibility is the unique automorphism sending θ_+ to θ_- since then $\sqrt{2} = \theta_+^2 - 2 \mapsto \theta_-^2 - 2 = -\sqrt{2}$, and so $\theta_- \mapsto \frac{-\sqrt{2}}{\theta_-} = -\theta_+$, so the order of this automorphism is 4.

4. *Let K/F be a Galois extension of degree n with $G = Gal(K/F)$. For $\alpha \in K$, define the norm and trace of α by*

$$N_{K/F}(\alpha) := \prod_{\sigma\in G}\sigma(\alpha), \qquad \textit{and} \qquad Tr_{K/F}(\alpha) = \sum_{\sigma\in G}\sigma(\alpha).$$

   Let $m_{\alpha,F}(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$.

   (a) Show that $N_{K/F}(\alpha) = (-1)^n a_0^{n/d}$ and $Tr_{K/F}(\alpha) = -\frac{n}{d}a_{d-1}$.
   Solution. Every Galois conjugate of α is $\sigma(\alpha)$ for precisely n/d values of σ. Therefore, $N_{K/F}(\alpha)$ is the (n/d)-th power of the product of the roots of $m_{\alpha,F}$, which is $(-1)^n a_0^{n/f}$. The result for the trace is similar.

   (b) Show that

$$N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta) \qquad \text{and} \qquad Tr_{K/F}(\alpha+\beta) = Tr_{K/F}(\alpha)+Tr_{K/F}(\beta).$$

   Solution.

$$N_{K/F}(\alpha\beta) = \prod_{\sigma\in G}\sigma(\alpha\beta) = \prod_{\sigma\in G}\sigma(\alpha)\sigma(\beta) = \prod_{\sigma\in G}\sigma(\alpha)\prod_{\sigma\in G}\sigma(\beta) = N_{K/F}(\alpha)N_{K/F}(\beta).$$

   The result for the trace is similar.

   (c) Show that $N_{K/F}(a\alpha) = a^n N_{K/F}(\alpha)$ and $Tr_{K/F}(a\alpha) = aTr_{K/F}(\alpha)$ for all $a \in F$, In particular show that $N_{K/F}(a) = a^n$ and $Tr_{K/F}(a) = na$ for all $a \in F$.
   Solution. $N_{K/F}(\alpha)$ is a product of n Galois conjugates of α, while $Tr_{K/F}(\alpha)$ is their sum. If $\sigma \in \mathrm{Gal}(K/F)$, then $\sigma(a\alpha) = a\sigma(\alpha)$, so when we multiply α by a, each Galois conjugate is multiplied by a. The formulas in the first sentence of the problem follow.

   The second sentence follows from the first, plus the fact that $N_{K/F}(1) = Tr_{K/F}(1) = 1$, since every automorphism fixes 1.

5. **Dummit and Foote #14.5.3:** *Determine the quadratic equation satisfied by the period $\alpha = \zeta_5 + \zeta_5^{-1}$ of the 5th root of unity ζ_5. Determine the quadratic equation satisfied by ζ_5 over $\mathbb{Q}(\alpha)$ and use this to explicitly solve for the 5th root of unity.*

   Solution. Let $\zeta := \zeta_5$. $\alpha^2 = \zeta^2 + \zeta^{-2} + 2 = 1 - \zeta - \zeta^{-1} = 1 - \alpha$ since the sum of all nth roots of unity is zero. Therefore, α is a root of the polynomial $x^2 + x - 1 \in \mathbb{Q}[x]$, and using the quadratic formula, $\alpha = \frac{-1 \pm \sqrt{5}}{2}$

   As is true for all n, ζ and ζ^{-1} are the roots of the polynomial $x^2 - \alpha x + 1 \in \mathbb{Q}(\alpha)[x]$, since the sum of ζ and ζ^{-1} is α, and their product is 1. Therefore, using the quadratic formula gives

$$\zeta = \frac{\alpha \pm \sqrt{\alpha^2 - 4}}{2} = \frac{\frac{-1 \pm \sqrt{5}}{2} \pm \sqrt{(\frac{-1 \pm \sqrt{5}}{2})^2 - 4}}{2} = \frac{-1 \pm \sqrt{5} \pm \sqrt{-10 \mp 2\sqrt{5}}}{4}.$$

   Here, the first $\pm$ and the $\mp$ must have opposite signs, and the two choices from this, plus the two choices from the second $\pm$, give all four primitive 5th roots of unity.

6. **Dummit and Foote #14.5.7:** *Show that complex conjugation restricts to the automorphism $\sigma_{-1} \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ of the cyclotomic field of nth roots of unity. Show that the field $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the subfield of real elements in $K = \mathbb{Q}(\zeta_n)$, called the maximal real subfield of K.*

   Solution. Let $\zeta := \zeta_n$ Since $|\zeta| = 1$, $\overline{\zeta} = \zeta^{-1}$. Since ζ is primitive over $\mathbb{Q}$, by the lemma in the previous homework solutions there exists an automorphism $\sigma_{-1} \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ sending $\zeta \mapsto \zeta^{-1}$, and this determines σ_{-1}. This means that complex conjugation restricted to $\mathbb{Q}(\zeta)$ must equal σ_{-1}, since they match on $\mathbb{Q}$ and ζ.

   Now, $\zeta + \zeta^{-1} = \zeta + \overline{\zeta} = 2\Re\zeta \in \mathbb{R}$, so $K^+ = \mathbb{Q}(\zeta + \zeta^{-1}) \subset \mathbb{R}$. On the other hand, $[K : K^+] = 2$ since ζ is a root of the polynomial $x^2 - (\zeta + \zeta^{-1})x + 1$, so there is no intermediate field strictly between K^+ and K. Since $K \not\subseteq \mathbb{R}$, K^+ is the maximal subfield of K, contained in $\mathbb{R}$, so it must equal the field $K \cap \mathbb{R}$ of all real elements of K.

7. **Dummit and Foote #14.5.10:** *Prove that $\mathbb{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic field over $\mathbb{Q}$.*

   Solution. Since $\mathbb{Q}(\sqrt[3]{2})$ has one, but not all of the roots of the separable polynomial $x^3 - 2$, the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois.

   Every cyclotomic field over $\mathbb{Q}$ is a Galois extension of $\mathbb{Q}$ with an abelian Galois group, and since every subgroup of an abelian group is normal, by the Fundamental Theorem of Galois theory, every subfield of a cyclotomic field is a Galois extension of $\mathbb{Q}$.