MATH 7211 Homework 5

Andrea Bourque

May 9, 2023

1 Problem 14.2.4

Let p be a prime. Determine the elements of the Galois group of $x^p - 2$.

Proof. The roots of $x^p - 2$ are of the form $\zeta^j\theta$, where $\zeta = \exp(2\pi i/p), \theta = \sqrt[p]{2} \in \mathbb{R}$, and $j = 0, 1, ..., p-1$. Therefore the splitting field of $x^p - 2$ is $\mathbb{Q}(\theta, \zeta)$. The minimal polynomial of θ is $x^p - 2$, since it is monic and irreducible by Eisenstein for prime 2. The minimal polynomial of ζ is $\Phi_p(x) = 1 + ... + x^{p-1}$. Thus the extensions $\mathbb{Q}(\theta)/\mathbb{Q}, \mathbb{Q}(\zeta)/\mathbb{Q}$ have degree p and $p-1$ respectively. Since these degrees are coprime, the degree of the extension $\mathbb{Q}(\theta, \zeta)/\mathbb{Q}$ is $p(p-1)$. Since $\mathbb{Q}(\theta, \zeta)$ is a splitting field of an irreducible polynomial over $\mathbb{Q}$, it is Galois, so the Galois group of $x^p - 2$ has order $p(p-1)$. The elements of the Galois group are automorphisms of $\mathbb{Q}(\theta, \zeta)$, which are determined by where the generators θ and ζ are sent. θ must be sent to a root of $x^p - 2$, and ζ must be sent to a root of $\Phi_p(x)$, which are of the form ζ^k where $k = 1, ..., p-1$. Then there are p choices for the image of θ and $p-1$ choices for the image of ζ, giving $p(p-1)$ choices. Since we already know the Galois group has $p(p-1)$ elements, each choice of image for θ and ζ gives an automorphism. Explicitly, the automorphisms are

$$\sigma_{jk} : \begin{cases} \theta \mapsto \zeta^j\theta \\ \zeta \mapsto \zeta^k \end{cases}$$

for $j \in \{0, 1, ..., p-1\}, k \in \{1, ..., p-1\}$. □

2 Problem 14.2.5

Let p be a prime. Prove that the Galois group of $x^p - 2$ is isomorphic to the group of matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ where $a, b \in \mathbb{F}_p, a \neq 0$.

Proof. In the previous exercise we saw that the elements of $\mathrm{Gal}(x^p - 2)$ are

$$\sigma_{jk} : \begin{cases} \theta \mapsto \zeta^j \theta \\ \zeta \mapsto \zeta^k \end{cases}$$

for $j \in \{0, 1, ..., p-1\}, k \in \{1, ..., p-1\}$. Since $\zeta^p = 1$, the j, k can be taken in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, with $k \neq 0$. Now, we demonstrate that the correspondence $f : \sigma_{jk} \mapsto \begin{pmatrix} k & j \\ 0 & 1 \end{pmatrix}$ is an isomorphism. First, we know $|\mathrm{Gal}(x^p - 2)| = p(p-1)$. The matrix group also has order $p(p-1)$, since there are $p-1$ choices for the top-left entry and p choices for the top-right entry, and no further relations. Thus it suffices to show that f is an injective homomorphism. That it is injective is clear, since $\begin{pmatrix} k & j \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ if and only if $k = 1, j = 0$, and σ_{01} is the identity automorphism. Now it remains to show f is a homomorphism. Matrix multiplication is the usual:

$$\begin{pmatrix} k & j \\ 0 & 1 \end{pmatrix} \begin{pmatrix} n & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} kn & km + j \\ 0 & 1 \end{pmatrix},$$

so it suffices to show $\sigma_{jk}\sigma_{mn} = \sigma_{km+j,kn}$. We have $\sigma_{jk}\sigma_{mn}(\theta) = \sigma_{jk}(\zeta^m\theta) = (\zeta^k)^m \zeta^j \theta = \zeta^{km+j}\theta = \sigma_{km+j,kn}(\theta)$, and $\sigma_{jk}\sigma_{mn}(\zeta) = \sigma_{jk}(\zeta^n) = (\zeta^k)^n = \zeta^{kn} = \sigma_{km+j,kn}(\zeta)$, so we are done. □

3 Problem 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 $\mathrm{Gal}(K/F_1) \cong \mathbb{Z}/8\mathbb{Z}, \mathrm{Gal}(K/F_2) \cong D_8, \mathrm{Gal}(K/F_3) \cong Q_8$.

Proof. Dummit and Foote Section 14.2 lays out the correspondence between subextensions of $K/\mathbb{Q}$ and subgroups of $\mathrm{Gal}(K/\mathbb{Q})$. In particular, with $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$, the book (along with the fundamental theorem of Galois theory) says that $\mathrm{Gal}(K/F_1) = \langle \sigma \rangle, \mathrm{Gal}(K/F_2) = \langle \sigma^2, \tau \rangle, \mathrm{Gal}(K/F_3) = \langle \sigma^2, \tau\sigma^3 \rangle$. We will show what these specific subgroups are isomorphic to.

Clearly $\langle \sigma \rangle$ is cyclic, and the order must divide 8, since $\sigma^8 = 1$. But $[K : \mathbb{Q}] = 16$ and $[F_1 : \mathbb{Q}] = 2$, so $[K : F_1] = 8$, so $\langle \sigma \rangle$ has order exactly 8. Hence it is isomorphic to the cyclic group of order 8.

We have $(\sigma^2)^4 = \tau^2 = 1$. We also have $(\sigma^2\tau)^2 = \sigma^2\tau\sigma^2\tau = \sigma\tau\sigma^3\sigma^2\tau = \tau\sigma^3\sigma^5\tau = \tau\sigma^8\tau = \tau^2 = 1$. In particular, $\sigma^2\tau = \tau^{-1}(\sigma^2)^{-1} = \tau(\sigma^2)^{-1}$. Thus $\langle \sigma^2, \tau \rangle$ contains the group $\langle a, b \mid a^4 = b^2 = 1, ab = ba^{-1} \rangle$, which is a presentation for D_8 (Dummit and Foote Section 1.2). But D_8 has order 8, and $\langle \sigma^2, \tau \rangle$ is the Galois group of K/F_2 which has degree $[K : \mathbb{Q}]/[F_2 : \mathbb{Q}] = 16/2 = 8$, so $\langle \sigma^2, \tau \rangle$ must be (isomorphic to) D_8.

We have $(\sigma^2)^4 = 1$, $(\tau\sigma^3)^2 = (\sigma\tau)^2 = \sigma\tau\sigma\tau = \sigma\tau^2\sigma^3 = \sigma^4 = (\sigma^2)^2$, and $(\tau\sigma^3)^{-1}\sigma^2\tau\sigma^3 = \sigma^5\tau^2\sigma^9 = \sigma^6 = (\sigma^2)^{-1}$. Then $\langle \sigma^2, \tau\sigma^3 \rangle$ contains the group $\langle a, b \mid a^4 = 1, b^2 = a^2, b^{-1}ab = a^{-1} \rangle$, which is a presentation for Q_8 (I searched every textbook I know, but the best I have for a source is "Topics in the Theory of Group Presentations" by D. L. Johnson). Again, the size of $\langle \sigma^2, \tau\sigma^3 \rangle$ is 8 by considering $[K : F_3] = [K : \mathbb{Q}]/[F_3 : \mathbb{Q}] = 16/2 = 8$, which is the same size as Q_8, so we are done. □

4 Problem 14.2.7

Determine all the subfields of the splitting field of $x^8 - 2$ which are Galois over $\mathbb{Q}$.

Proof. Of course, we have the whole splitting field $\mathbb{Q}(\sqrt[8]{2}, i)$ and the base field $\mathbb{Q}$. By the fundamental theorem of Galois theory, it suffices to determine the normal subgroups of $\mathrm{Gal}(x^8 - 2)$. Dummit and Foote section 14.2 contains the lattice of subgroups of $\mathrm{Gal}(x^8 - 2) = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$, so we just have to make the routine check of which ones are normal, and then use the book's subgroup-subfield correspondence to give the subfields. Finally, before we begin, recall that, given a finitely generated group and a finitely generated subgroup, it suffices to check normality by generators of the group on generators of the subgroup.

1. $\langle \sigma^2, \tau \rangle$. Clearly conjugation by σ and τ fixes σ^2 and τ respectively. Then we have $\tau\sigma^2\tau = \tau^2\sigma^6 = (\sigma^2)^{-1}$, which is in the subgroup. Finally we have $\sigma\tau\sigma^{-1} = \tau\sigma^3\sigma^{-1} = \tau\sigma^2$, which is in the subgroup. So this one is normal.

2. $\langle \sigma \rangle$. Clearly invariant under σ conjugation, and $\tau\sigma\tau = \tau^2\sigma^3 = \sigma^3 \in \langle \sigma \rangle$, so this is normal.

3. $\langle \sigma^2, \tau\sigma^3 \rangle$. The first generator is invariant under σ conjugation. We have $\tau\sigma^2\tau = (\sigma^2)^{-1}$ which is in the group. For the second generator we have $\tau\tau\sigma^3\tau = \sigma^3\tau = \tau\sigma^9 = \tau\sigma = \tau\sigma^3(\sigma^2)^{-1}$ is in the subgroup, and $\sigma\tau\sigma^3\sigma^{-1} = \tau\sigma^3\sigma^2$ is in the subgroup. Thus this one is normal.

4. $\langle \sigma^4, \tau\sigma^6 \rangle$. We have $\sigma\tau\sigma^6\sigma^{-1} = \tau\sigma^8 = \tau$. If τ was in this subgroup, then we would have σ^2 and hence we would be in $\langle \sigma^2, \tau \rangle$. Since we know these are distinct (according to the diagram in Dummit and Foote), this shows that this subgroup is not normal.

5. $\langle \sigma^4, \tau \rangle$. We have $\sigma\tau\sigma^{-1} = \tau\sigma^2$. If this was in the subgroup, then we would have σ^2, and then we would be in $\langle \sigma^2, \tau \rangle$ as in the previous case. Thus this subgroup is not normal.

6. $\langle \sigma^2 \rangle$. Clearly invariant under σ conjugation, and $\tau\sigma^2\tau = \tau^2\sigma^6 = (\sigma^2)^3$ is in the subgroup, so this is normal.

7. $\langle \tau\sigma^3 \rangle$. Note that $(\tau\sigma^3)^2 = \tau\sigma^3\tau\sigma^3 = \tau^2\sigma^{12} = \sigma^4$, $(\tau\sigma^3)^3 = \tau\sigma^7, (\tau\sigma^3)^4 = (\sigma^4)^2 = 1$, and these are all the elements in the group. Conjugation by τ gives $\tau\tau\sigma^3\tau = \sigma^3\tau = \tau\sigma^9 = \tau\sigma$ which is not an element, so the subgroup is not normal.

8. $\langle \tau\sigma \rangle$. Note that $\tau\tau\sigma\tau = \sigma\tau = \tau\sigma^3$ cannot be in the group, as $\langle \tau\sigma^3 \rangle$ does not contain $\tau\sigma$ as we saw above. This subgroup is not normal.

9. $\langle \tau\sigma^2 \rangle$. Conjugation by τ gives $\sigma^2\tau = \tau\sigma^6$. But $(\tau\sigma^2)^2 = \tau\sigma^2\tau\sigma^2 = \tau^2\sigma^8 = 1$, so the only elements of $\langle \tau\sigma^2 \rangle$ are 1 and $\tau\sigma^2$. This subgroup is not normal.

10. A similar line of reasoning shows that the order 2 subgroups $\langle \tau\sigma^6 \rangle, \langle \tau\sigma^4 \rangle, \langle \tau \rangle$ are not normal.

11. $\langle \sigma^4 \rangle$. This is normal because $\tau\sigma^4\tau = \tau^2\sigma^{12} = \sigma^4$.

To recap, we have the normal subgroups are $\langle \sigma^2, \tau \rangle, \langle \sigma \rangle, \langle \sigma^2, \tau\sigma^3 \rangle, \langle \sigma^2 \rangle, \langle \sigma^4 \rangle$. Comparing the subgroup lattice to the subfield lattice (again, pictured in Dummit and Foote), we see that the (proper and nontrivial) subfields of the splitting field of $x^8 - 2$ which are Galois over $\mathbb{Q}$ are (respectively): $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(i, \sqrt{2})$, and $\mathbb{Q}(i, \sqrt[4]{2})$. □

5 Problem 14.2.14

Show that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a cyclic quartic field, i.e. a Galois extension with Galois group $\mathbb{Z}/4\mathbb{Z}$.

Proof. Let $\alpha = \sqrt{2+\sqrt{2}}$. Then $\alpha^2 - 2 = \sqrt{2}$, so $(\alpha^2-2)^2 - 2 = 0$. The polynomial $p(x) = (x^2-2)^2 - 2 = x^4 - 4x^2 + 2$ is irreducible by Eisenstein for the prime 2, so it is the minimal polynomial for α over $\mathbb{Q}$. Thus $\mathbb{Q}(\alpha)$ is a degree 4 extension. Writing $p(x) = (x^2-2)^2 - 2$ allows one to find all the roots of $p(x)$; namely, they are $\alpha, -\alpha, \beta := \sqrt{2-\sqrt{2}}$, and $-\beta$. Clearly $\alpha, -\alpha \in \mathbb{Q}(\alpha)$. It suffices to show $\beta \in \mathbb{Q}(\alpha)$. But $\alpha^2 - 2 = \sqrt{2} \in \mathbb{Q}(\alpha)$, and $\alpha\beta = \sqrt{2}$, so $\beta = \alpha - 2\alpha^{-1} \in \mathbb{Q}(\alpha)$. Thus $p(x)$ splits in $\mathbb{Q}(\alpha)$. Since $\mathbb{Q}(\alpha)$ is generated by the roots (even just one root) of $p(x)$, it follows that $\mathbb{Q}(\alpha)$ is a splitting field for $p(x)$. We have demonstrated that $p(x)$ has distinct roots, so $\mathbb{Q}(\alpha)$ is a Galois extension.

We know that $|\mathrm{Gal}(\mathbb{Q}(\alpha))| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. The only groups of order 4 are the cyclic group of order 4 and the Klein-4 group $(\mathbb{Z}/2\mathbb{Z})^2$ (as a brief justification, there is a simple lemma that a group of order square of a prime is abelian, and then we apply the classification of finite abelian groups). The latter group lacks an element of order 4, so it suffices to give an automorphism of $\mathbb{Q}(\alpha)$ of order 4. As The automorphism must permute the roots $\alpha, -\alpha, \beta, -\beta$ in a way that preserves the algebraic relations $\alpha + (-\alpha) = 0, \beta + (-\beta) = 0, \beta = \alpha - 2\alpha^{-1}$. These three relations imply that an automorphism is completely determined by the image of α. We know a priori that there are four automorphisms, and since there are four roots as possible images of α, each image must give an automorphism. Take the automorphism σ for which $\sigma\alpha = \beta$. Then $\sigma\beta = \beta - 2\beta^{-1} = \frac{-\sqrt{2}}{\sqrt{2-\sqrt{2}}} = -\alpha$. In particular, $\sigma^2\alpha = -\alpha, \sigma^3\alpha = -\beta, \sigma^4\alpha = \alpha$. Thus σ has order 4, proving that $\mathrm{Gal}(\mathbb{Q}(\alpha))$ is cyclic of order 4. □