Algebra II: Complementary exercises on Galois groups

April 29, 2022

Problem 1 (Computing Galois groups)**.** Compute $G(L) = \mathrm{Aut}_{\mathbb{Q}}(L)$, list all subgroups H of $G(L)$ and determine the corresponding intermediate field L^H for each of the following field extensions L over $\mathbb{Q}$:

1. $L = \mathbb{Q}(\sqrt[3]{2})$,
2. $L = \mathbb{Q}(\sqrt[4]{2})$,
3. L is the splitting field of $x^8 - 1$ over $\mathbb{Q}$,
4. L is the splitting field of $x^3 - 2$ over $\mathbb{Q}$.
5. $L = \mathbb{Q}(e^{2\pi i/5})$,
6. $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
7. L is the splitting field of $x^4 + 1$ over $\mathbb{F}_3$.
8. $L = \mathbb{Q}(i + \sqrt{2})$.

Solution. 1. Suppose that $L = \mathbb{Q}(\sqrt[3]{2})$. Note that $\sqrt[3]{2}$ is the root of the monic irreducible polynomial x^3-2 over $\mathbb{Q}$. The roots of x^3-2 in L are $\sqrt[3]{2}$. The group $\mathrm{Aut}_{\mathbb{Q}}(L)$ is trivial, has no non-trivial subgroups, and the field extension has no intermediate fields.

2. Suppose that $L = \mathbb{Q}(\sqrt[4]{2})$. Note that $\sqrt[4]{2}$ is the root of the monic irreducible polynomial x^4-2 over $\mathbb{Q}$. The roots of x^4-2 in L are $\pm\sqrt[4]{2}$, so any non-trivial $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(L)$ must map $\sqrt[4]{2}$ to $-\sqrt[4]{2}$. We write $\mathrm{Aut}_{\mathbb{Q}}(L) = \{id, \sigma\}$; in particular, $|\mathrm{Aut}_{\mathbb{Q}}(L)| = 2$.[1] There is only one group of order 2, so $\mathrm{Aut}_{\mathbb{Q}}(L) \cong \mathbb{Z}_2$. The two subgroups of G are G and $\{id\}$. By considering the basis $\{1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{8}\}$ of L over $\mathbb{Q}$, one can easily see that $L^G = \mathbb{Q}(\sqrt{2})$ and $L^{\{id\}} = L$.

3. Suppose that L is the splitting field of x^8-1. Since $x^8-1 = (x-1)(x+1)(x^2+1)(x^4+1)$, $L = \mathbb{Q}(\zeta_8)$ where $\zeta_8 = \sqrt{2}/2 + i\sqrt{2}/2$ is a primitive 8th root of unity. It is a Galois extension since it is the splitting field of x^8-1 over a perfect field. The Galois group $\mathrm{Aut}_{\mathbb{Q}}(L)$ is isomorphic to the group $(\mathbb{Z}/8\mathbb{Z})^\times = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. We omit the discussion on trivial subgroups. It has 3 non-trivial subgroups, that are cyclic of order 2. One is generated by the automorphism σ_3 sending ζ_8 to ζ_8^3. Notice that $\zeta_8 + \zeta_8^3$ is fixed by the automorphism. Thus, the quadratic subfield $\mathbb{Q}(\sqrt{-2})$ is fixed by this automorphism. Then, by Galois correspondence, this subfield is the corresponding fixed field of the subgroup generated by σ_3. The analysis of the other two cases should be similar. We omit it.

4. This was discussed during the lectures, but we will go over some of the details again. Suppose that L is the splitting field of x^3-2 over $\mathbb{Q}$. We know that $L = \mathbb{Q}(\omega, \sqrt[3]{2})$, where $\omega = \exp(2\pi i/3)$. This is clearly a Galois extension. Since it is of degree 6, G is of order 6, say $G = \{id, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$. There are two non-isomorphic groups of order 6: $\mathbb{Z}/6\mathbb{Z}$ and S_3. The first is cyclic (and hence abelian), and the other is the permutation group on 3 elements (which is not abelian). To distinguish them, we can compute orders ($\mathbb{Z}/6\mathbb{Z}$ has an element of order 6 but S_3 does not!). The elements of $\mathrm{Aut}_{\mathbb{Q}}(L)$ are completely determined by their action on $\sqrt[3]{2}$ and ω; furthermore this action must send roots of x^3-2 (and roots of x^3-1) to roots of x^3-2 (to roots of x^3-1 respectively). Therefore, the five non-trivial $\mathbb{Q}$-automorphisms of L are:

$$\begin{aligned} \sigma_1(\sqrt[3]{2}) &= \sqrt[3]{2}\omega, & \sigma_2(\sqrt[3]{2}) &= \sqrt[3]{2}\omega^2, & \sigma_3(\sqrt[3]{2}) &= \sqrt[3]{2}, \\ \sigma_1(\omega) &= \omega, & \sigma_2(\omega) &= \omega, & \sigma_3(\omega) &= \omega^2, \\ \sigma_4(\sqrt[3]{2}) &= \sqrt[3]{2}\omega, & \sigma_5(\sqrt[3]{2}) &= \sqrt[3]{2}\omega^2, \\ \sigma_4(\omega) &= \omega^2, & \sigma_5(\omega) &= \omega^2. \end{aligned}$$

A short calculation shows that $|\sigma_1| = 3$, $|\sigma_2| = 3$, $|\sigma_3| = 2$, $|\sigma_4| = 2$, and $|\sigma_5| = 2$. Thus, $\mathrm{Gal}_{\mathbb{Q}}(L) \simeq S_3$. Since the non-trivial subgroups of S_3 are of order 2 or 3, they

[1] Here, $|\mathrm{Aut}_{\mathbb{Q}}(L)| = 2 < 4 = [L : K]$, which confirms that this extension is not Galois.

should be cyclic groups. Explicitly:

$$G_1 = \langle \sigma_1 \rangle = \{id, \sigma_1, \sigma_2\}.$$
$$G_2 = \langle \sigma_2 \rangle = \{id, \sigma_2, \sigma_1\}.$$
$$G_i = \langle \sigma_i \rangle = \{id, \sigma_i\}, \text{ for } i = 3, 4, 5.$$

It is not surprising that $G_1 = G_2$, since $\sigma_1^2 = \sigma_2$, and $\mathbb{Z}_3$ has two generators. Hence, G has six subgroups (4 non-trivial subgroups). Since the extension is Galois, we know what the fixed fields for the trivial subgroups G and $\{1\}$ are. To compute the fixed fields for the non-trivial subgroups, pick a suitable basis of L. Then, one can show that $L^{G_1} = \mathbb{Q}(\omega)$, $L^{G_3} = \mathbb{Q}(\sqrt[3]{2})$, $L^{G_4} = \mathbb{Q}(\sqrt[3]{2}\omega^2)$, $L^{G_5} = \mathbb{Q}(\sqrt[3]{2}\omega)$.

5. Suppose that $L = \mathbb{Q}(e^{2\pi i/5})$. L is the 5th cyclotomic field which is Galois over $\mathbb{Q}$. Its Galois group is isomorphic to $(\mathbb{Z}/5\mathbb{Z})^\times$. So it is a cyclic group of order 4 since $\mathbb{Z}/5\mathbb{Z}$ is a finite field, which consists of the automorphisms sending $e^{2\pi i/5}$ to other 5th primitive roots of unity. It has two trivial subgroups, i.e., the trivial group and itself. You can easily compute their fixed fields. Its only non-trivial subgroup is a subgroup of order 2. By Galois correspondence, it corresponds to a quadratic extension over $\mathbb{Q}$. Since $e^{2\pi i/5} + e^{-2\pi i/5} = 2\cos(2\pi i/5) = -1/2 + \sqrt{5}/2$. This quadratic extension is $\mathbb{Q}(\sqrt{5})$.

6. Suppose that $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Since L is the splitting field of $(x^2-2)(x^2-3)$ over a perfect field $\mathbb{Q}$, $L/\mathbb{Q}$ is Galois. You can easily find that the Galois group is generated by two automorphisms σ_2, σ_3 where σ_2 sends $\sqrt{2}$ to $-\sqrt{2}$ and fixes $\sqrt{3}$ and σ_3 fixes $\sqrt{2}$ and sends $\sqrt{3}$ to $-\sqrt{3}$. Thus, the Galois group is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. For two trivial subgroups, the descriptions are similar. It has another three subgroups of order 2, which are generated by σ_2, σ_3, and $\sigma_2\sigma_3$, respectively. By Galois correspondence, the corresponding fixed subfields are $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\sqrt{6})$.

7. Suppose that L is the splitting field of x^4+1 over $\mathbb{F}_3$. First, you easily check that x^4+1 is irreducible over $\mathbb{F}_3$. So, the splitting field of x^4+1 over $\mathbb{F}_3$ is simply adding a root of x^4+1 to $\mathbb{F}_3$. Thus, $L/\mathbb{F}_3$ is of degree 4. The Galois group by our discussion of finite fields, must be a cyclic group of order 4, which is generated by the Frobenius automorphism $\sigma\colon x \mapsto x^3$. We omit the discussion of trivial subgroups. Thus, the only non-trivial subgroup is cyclic of order 2, which is generated by $\sigma^2\colon x \mapsto x^9$. The fixed field is obviously seen to be $\mathbb{F}_9$ under the identification.

8. Note that $\sqrt{2} + i$ is a root of the irreducible polynomial $f(x) = x^4 - 2x^2 + 9$, so $[L : K] = 4$. Furthermore, f splits completely in L so L is a splitting field for f over $\mathbb{Q}$. Since $\mathbb{Q}$ is a perfect field, this implies that $L : K$ is a Galois extension, and so

$G = \mathrm{Aut}_{\mathbb{Q}}(L)$ has order 4. Explicitly, $G = \{Id, \sigma_1, \sigma_2, \sigma_3\}$ where

$$\begin{array}{ccc} \sigma_1(i) = i, & \sigma_2(i) = -i, & \sigma_3(i) = -i, \\ \sigma_1(\sqrt{2}) = -\sqrt{2}, & \sigma_2(\sqrt{2}) = \sqrt{2}, & \sigma_3(\sqrt{2}) = -\sqrt{2}. \end{array}$$

In particular, each of the automorphisms σ_i has order 2, so $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. The proper subgroups of G are isomorphic to $\mathbb{Z}_2$; explicitly they are $G_1 = \{Id, \sigma_1\}, G_2 = \{Id, \sigma_2\}, G_3 = \{Id, \sigma_3\}$. In order to compute L^{G_i}, we choose a convenient basis for elements in L. It is easy to see that the set $\{1, \sqrt{2}, i, i\sqrt{2}\}$ is a $\mathbb{Q}$-basis of L. Then:

$$L^{G_1} = \mathbb{Q}(i), \quad L^{G_2} = \mathbb{Q}(\sqrt{2}), \quad \text{and} \quad L^{G_3} = \mathbb{Q}(i\sqrt{2}).$$