MATH6303 Modern Algebra II
Homework III

Joel Sleeba

March 2, 2025

1. **Solution:** We know that the roots of $x^p - 2$ are precisely, $2^{\frac{1}{p}}e^{i\frac{2\pi j}{p}}$, where $0 \leq j \leq p-1$. Hence the splitting field of $x^p - 2$ is $\mathbb{Q}(2^{\frac{1}{p}}, e^{i\frac{2\pi}{p}})$. Since $2^{\frac{1}{p}}$ is a root of the irreducible (by Eisenstein with 2) polynomial $x^p - 2$, and $e^{i\frac{2\pi}{p}}$ is a root of the irreducible cyclotomic polynomial $x^{p-1} + x^{p-2} + \ldots + x + 1$, we see that the degree of the extension

$$[\mathbb{Q}(2^{\frac{1}{p}}, e^{i\frac{2\pi}{p}}) : \mathbb{Q}] = [\mathbb{Q}(2^{\frac{1}{p}}, e^{i\frac{2\pi}{p}}) : \mathbb{Q}(2^{\frac{1}{p}})][\mathbb{Q}(2^{\frac{1}{p}}) : \mathbb{Q}] = p(p-1)$$

Hence the Galois group, $\mathrm{Aut}(\mathbb{Q}(2^{\frac{1}{p}}, e^{i\frac{2\pi}{p}})/\mathbb{Q})$ has $p(p-1)$ elements, where each $\tau \in \mathrm{Aut}(\mathbb{Q}(2^{\frac{1}{p}}, e^{i\frac{2\pi}{p}})/\mathbb{Q}$ is uniquely determined by the image of $2^{\frac{1}{p}}$, and $e^{i\frac{2\pi}{p}}$. Also notice that for any $\tau \in \mathrm{Aut}(\mathbb{Q}(2^{\frac{1}{p}}, e^{i\frac{2\pi}{p}})/\mathbb{Q})$,

$$\begin{aligned} \tau(2^{\frac{1}{p}}) &\in \{2^{\frac{1}{p}}e^{i\frac{2\pi j}{p}} \ : \ 0 \leq j < p\} \\ \tau(e^{i\frac{2\pi}{p}}) &\in \{e^{i\frac{2\pi j}{p}} \ : \ 0 < j < p\} \end{aligned}$$

We claim that $\mathrm{Aut}(\mathbb{Q}(2^{\frac{1}{p}}, e^{i\frac{2\pi}{p}})/\mathbb{Q})$ is generated by the two automorphisms, τ_1, τ_2, where

$$\begin{aligned} \tau_1(2^{\frac{1}{p}}) = 2^{\frac{1}{p}}e^{i\frac{2\pi}{p}},\ \tau_1(e^{i\frac{2\pi}{p}}) = e^{i\frac{2\pi}{p}} \\ \tau_2(2^{\frac{1}{p}}) = 2^{\frac{1}{p}},\ \tau_2(e^{i\frac{2\pi}{p}}) = e^{i\frac{4\pi}{p}} \end{aligned}$$

and then further extended to the whole field $\mathbb{Q}(2^{\frac{1}{p}}, e^{i\frac{2\pi}{p}})$. To see this, if $\tau \in \mathrm{Aut}(\mathbb{Q}(2^{\frac{1}{p}}, e^{i\frac{2\pi}{p}})/\mathbb{Q})$ such that $\tau(2^{\frac{1}{p}}) = 2^{\frac{1}{p}}e^{i\frac{2\pi j}{p}}$, and $\tau(e^{i\frac{2\pi}{p}}) = e^{i\frac{2\pi k}{p}}$, then we can verify that $\tau = \tau_1^j\tau_2^k$. It is easy to see that τ_1^p is the identity automorphism. We can also verify that, $\tau_2^{p-1}(e^{i\frac{2\pi}{p}}) = e^{i\frac{2\pi}{p}}$. Thus we get that

$$\mathrm{Aut}(\mathbb{Q}(2^{\frac{1}{p}}, e^{i\frac{2\pi}{p}})/\mathbb{Q}) = \langle \tau_1, \tau_2 : \tau_1^p = 1 = \tau_2^{p-1}, \tau_1\tau_2 = \tau_2\tau_1^2 \rangle$$

Now we notice that for the given matrix group, the matices $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and $B = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ generate the whole matrix as

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^m = \begin{pmatrix} 2^m & 0 \\ 0 & 1 \end{pmatrix}$$

and since any element in $\mathbb{F}_p$ has a form 2^m, we get

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2^m & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2^m & n \\ 0 & 1 \end{pmatrix}$$

Again we see that $|A| = p$, and Fermat's little theorem give $|B| = p - 1$. Moreover, observing $AB = BA^2$, we see that $\langle A, B \rangle$, satisfy all the relations of the above group and hence we see that they are isomorphic.

2. **Solution:** We notice that the roots of $x^2 - 14x + 9$ are $7 \pm \sqrt{40}$ using the quadratic formula. Hence the roots of $x^4 - 14x^2 + 9$ are precisely $\pm\sqrt{7 \pm \sqrt{40}}$. Moreover, notice that

$$\sqrt{7 + \sqrt{40}} \times \sqrt{7 - \sqrt{40}} = \sqrt{7^2 - 40} = \sqrt{9} = 3 \tag{1}$$

Hence the splitting field of the polynomial is $K = \mathbb{Q}(\sqrt{7 + \sqrt{40}})$. Thus $[\mathbb{Q}(\sqrt{7 + \sqrt{10}}) : \mathbb{Q}] \leq 4$. Hence the Galois group of the splitting field is of order ≤ 4. Now let $\tau \in \mathrm{Aut}(K/\mathbb{Q})$. Then $\tau(\sqrt{7 + \sqrt{40}})$ can be mapped to one of $\pm\sqrt{7 \pm \sqrt{40}}$. Since each of them give distinct automorphisms, we see that the Galois group contain atleast 4 distinct automorphisms. This combined with the above inference, we get that $\mathrm{Aut}(K/\mathbb{Q})$ has exactly 4 elements.

Let's look at these by cases. If τ fixes $\sqrt{7 + \sqrt{40}}$, since $\sqrt{7 - \sqrt{40}} = \frac{3}{\sqrt{7+\sqrt{40}}}$, it fixes $\sqrt{7 - \sqrt{40}}$ and therefore the whole K, and becomes just the identity map. By the same reasoning, any element of $\mathrm{Aut}(K/\mathbb{Q})$ which fixes either of $\pm\sqrt{7 \pm \sqrt{40}}$ fixes the whole field K.

Let $\tau(\sqrt{7 + \sqrt{40}}) = \sqrt{7 - \sqrt{40}}$, then by Equation 1, $\tau(\sqrt{7 - \sqrt{40}}) = \sqrt{7 + \sqrt{40}}$. This forces $\tau^2 = e$.

Now let $\tau(\sqrt{7 + \sqrt{40}}) = -\sqrt{7 - \sqrt{40}}$, then again Equation 1 forces $\tau(\sqrt{7 - \sqrt{40}}) = -\sqrt{7 + \sqrt{40}}$. Thus, again $\tau^2 = e$.

By a similar reasoning, we'll get that $\tau(\sqrt{7+\sqrt{40}}) = -\sqrt{7+\sqrt{40}}$ also gives $\tau^2 = e$.

Since we exhausted all the possible automorphisms, we see that $\tau^2 = e$ for all $\tau \in \operatorname{Aut}(K/\mathbb{Q})$. Hence the Galois group must be isomorphic to V_4.

3. **Solution:** We get that $x^4 - 4x^2 + 2$ is an irreducible polynomial (Eisenstein with $p = 2$) with root $\sqrt{2+\sqrt{2}}$. All roots of $x^4 - 4x^2 + 2$ are $\pm\sqrt{2 \pm \sqrt{2}}$. Moreover,

$$\sqrt{2+\sqrt{2}} \times \sqrt{2-\sqrt{2}} = \sqrt{2}$$

shows that the splitting field of x^4-4x^2+2, is $K = \mathbb{Q}(\sqrt{2+\sqrt{2}}, \sqrt{2})$. Moreover we notice that $\sqrt{2+\sqrt{2}} \notin \mathbb{Q}(\sqrt{2})$, while $\sqrt{2+\sqrt{2}}$ is a root of the polynomial $x^2 - (2+\sqrt{2})$, which is again irreducible (by having no roots) in $\mathbb{Q}(\sqrt{2})$. Thus we get that

$$[\mathbb{Q}(\sqrt{2+\sqrt{2}}, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2+\sqrt{2}}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4$$

Thus we see that the Galois group of $x^4 - 4x^2 + 2$ is of order 4. Now consider $\tau \in \operatorname{Aut}(K/\mathbb{Q})$ such that

$$\tau(\sqrt{2+\sqrt{2}}) = \sqrt{2-\sqrt{2}}, \text{ and } \tau(\sqrt{2-\sqrt{2}}) = -\sqrt{2+\sqrt{2}}$$

We notice that the above definition gives $\tau(2+2) = 2+2$, which in turn fixes every $r \in \mathbb{Q}$. Thus τ extends to a well defined automorphism of K, which fixes $\mathbb{Q}$. Then it is easy to verify that $|\tau| = 4$. Thus we see that $\operatorname{Gal}(K/\mathbb{Q}) = \mathbb{Z}_4$.

4. **Solution:** Let K be the splitting field of the polynomial $x^p - x - a$. Since this is a polynomial of p degrees, it can have atmost p roots in K. Let $\alpha \in K$ be a root. Then $\alpha^p - \alpha - a = 0$. We observe that $\alpha + 1$ is also a root since $(\alpha+1)^p = \alpha^p + 1$ in a field of characteristic p, and

$$(\alpha+1)^p - (\alpha+1) - a = (\alpha^p + 1) - (\alpha+1) - a = \alpha^p - \alpha - a = 0$$

Thus we see that if α is a root of the polynomial, then $\alpha + i$ is a root for all $0 < i < p$. Moreover all of them are distict since $\alpha+i = \alpha+j$ iff $p|i-j$. Hence $\alpha, \alpha+1, \alpha+2, \ldots \alpha+p-1$ are all the roots of the polynomial $x^p - x - a$. Thus we see that the splitting field, $K = \mathbb{F}_p(\alpha)$.

We know that the Galois group $\mathrm{Aut}(K/\mathbb{F}_p)$ permutes the roots of the polynomial $x^p - x - a$. Since all the roots of $x^p - x - a$ are of the form $\alpha + i$, where $i \in \mathbb{F}_p$, $\tau \in \mathrm{Aut}(K/\mathbb{F}_p)$ is uniquely determined by $\tau(\alpha)$. Let $\tau_1 \in \mathrm{Aut}(K/\mathbb{F}_p)$ such that $\tau(\alpha) = \alpha + 1$. We claim that $\mathrm{Aut}(K/\mathbb{F}_p) = \langle \tau_1 : \tau_1^p = 1 \rangle$. If $\tau_i \in \mathrm{Aut}(K/\mathbb{F}_p)$ such that $\tau_i(\alpha) = \alpha + i$, then $\tau_i = (\tau_1)^i$. Thus the automorphism group is generated by τ_1, and therefore it is cyclic.