Mathematics 352 – Abstract Algebra II
Solutions for Problem Set 8
March 31, 2008

Section 11.1

11. $K = \mathbb{Q}(\sqrt{2}, i)$ is the splitting field over $\mathbb{Q}$ of the polynomial $f(x) = (x^2 - 2)(x^2 + 1)$. The same "two-step" argument done in class and in Example 2.A on page 374-375 of the text shows that there are elements of $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, i)$ acting on the generators as follows:

$$\begin{aligned}
\mathrm{id} : \sqrt{2} &\mapsto \sqrt{2} \\
i &\mapsto i \\
\alpha : \sqrt{2} &\mapsto -\sqrt{2} \\
i &\mapsto i \\
\beta : \sqrt{2} &\mapsto \sqrt{2} \\
i &\mapsto -i \\
\gamma : \sqrt{2} &\mapsto -\sqrt{2} \\
i &\mapsto -i
\end{aligned}$$

(Recall this works because for each action on $\sqrt{2}$, K is still the splitting field of $x^2 + 1$ over $\mathbb{Q}(\sqrt{2})$ so we can extend either action on $\sqrt{2}$ to each possible action on i using Corollary 10.8 (the "Key Corollary" of Theorem 10.7). This yields a Galois group isomorphic to the Klein 4-group $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ since $\gamma = \beta \circ \alpha$ and α, β, γ all have order 2.

12. The idea is similar to what happened above in Exercise 11 and Example 2.A. Applying a "three-step" argument, we have elements of $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ as follows:

$$\begin{aligned}
\mathrm{id} : \sqrt{2} &\mapsto \sqrt{2} \\
\sqrt{3} &\mapsto \sqrt{3} \\
\sqrt{5} &\mapsto \sqrt{5} \\
\alpha_{100} : \sqrt{2} &\mapsto -\sqrt{2} \\
\sqrt{3} &\mapsto \sqrt{3} \\
\sqrt{5} &\mapsto \sqrt{5} \\
\alpha_{010} : \sqrt{2} &\mapsto \sqrt{2} \\
\sqrt{3} &\mapsto -\sqrt{3} \\
\sqrt{5} &\mapsto \sqrt{5} \\
\alpha_{001} : \sqrt{2} &\mapsto \sqrt{2} \\
\sqrt{3} &\mapsto \sqrt{3} \\
\sqrt{5} &\mapsto -\sqrt{5}
\end{aligned}$$

$$\begin{aligned}
\alpha_{110} : \sqrt{2} &\mapsto -\sqrt{2} \\
\sqrt{3} &\mapsto -\sqrt{3} \\
\sqrt{5} &\mapsto \sqrt{5} \\
\alpha_{101} : \sqrt{2} &\mapsto -\sqrt{2} \\
\sqrt{3} &\mapsto \sqrt{3} \\
\sqrt{5} &\mapsto -\sqrt{5} \\
\alpha_{011} : \sqrt{2} &\mapsto \sqrt{2} \\
\sqrt{3} &\mapsto -\sqrt{3} \\
\sqrt{5} &\mapsto -\sqrt{5} \\
\alpha_{111} : \sqrt{2} &\mapsto -\sqrt{2} \\
\sqrt{3} &\mapsto -\sqrt{3} \\
\sqrt{5} &\mapsto -\sqrt{5}
\end{aligned}$$

By examining the composition table for these $\mathbb{Q}$-automorphisms, we see that they form an abelian group of order 8 in which every element other than id has order 2. By the structure theorem for finite abelian groups this means that $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

15. (a) If $\sigma : \mathbb{R} \to \mathbb{R}$ is an automorphism, then for all $x \in \mathbb{R}$, $\sigma(x^2) = \sigma(x \cdot x) = \sigma(x) \cdot \sigma(x) = (\sigma(x))^2$. If $x \neq 0$, then $\sigma(x) \neq 0$ since σ is one-to-one. Therefore if $a > 0$, then we can write $\sigma(a) = \sigma(x^2) = (\sigma(x))^2$ in $\mathbb{R}$. Therefore $\sigma(a)$ is the square of a nonzero real number, hence is strictly positive. It follows that σ takes positive elements of $\mathbb{R}$ to positive elements of $\mathbb{R}$.

(b) If $a, b \in R$ and $\sigma \in \mathrm{Gal}_{\mathbb{Q}}\mathbb{R}$, suppose $a < b$. Then $b - a > 0$, so by part (a), we have $\sigma(b-a) > 0$. But $\sigma(b-a) = \sigma(b) - \sigma(a) > 0$ since σ is an automorphism of $\mathbb{R}$. It follows that $\sigma(b) > \sigma(a)$, or equivalently $\sigma(a) < \sigma(b)$. (In other words, σ is *order-preserving*.)

(c) Now suppose that $c < r < d$ with $c, d \in \mathbb{Q}$ and $r \in \mathbb{R}$. If $\sigma \in \mathrm{Gal}_{\mathbb{Q}}\mathbb{R}$, then part (b) shows $\sigma(c) < \sigma(r) < \sigma(d)$. But $c, d \in \mathbb{Q}$, so $\sigma(c) = c$ and $\sigma(d) = d$. Therefore $c < \sigma(r) < d$, and we have:

$$c < r < d \Rightarrow c < \sigma(r) < d \tag{1}$$

whenever $c, d \in \mathbb{Q}$. We claim that this implies $\sigma(r) = r$ for all $r \in \mathbb{R}$, and hence $\sigma = \mathrm{id}$. The reason this is true is that given any $\varepsilon > 0$ and $r \in R$, there exist rational numbers $d \in (r, r+\varepsilon)$ and $c \in (r-\varepsilon, r)$. If we apply (1) with such c, d, then we see $r - \varepsilon < \sigma(r) < r + \varepsilon$. Since we can do this for all $\varepsilon > 0$, $\sigma(r) = r$.

16. When ζ satisfies the condition in this problem (that the powers of ζ are n *distinct* solutions of $x^n - 1 = 0$), we say that ζ is a *primitive nth root of one*. In the irreducible factorization of $x^n - 1$ in $\mathbb{Q}[x]$, suppose that ζ is a root of the irreducible polynomial $p(x)$. Then by Theorem 11.3, if $\sigma \in \mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\zeta)$, then $\sigma(\zeta)$ is also a root of $p(x)$. However this means that $\sigma(\zeta) = \zeta^k$ for some $k \in \{1, \ldots, n\}$. Now suppose $\tau \in \mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\zeta)$ is another element of the Galois group. By the same

reasoning $\tau(\zeta) = \zeta^\ell$ for some $\ell \in \{1, \ldots, n\}$. But now consider the composition $\sigma \circ \tau$:

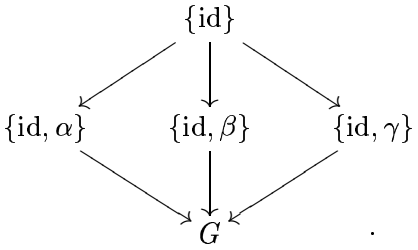
$$(\sigma \circ \tau)(\zeta) = \sigma(\tau(\zeta)) = \left(\zeta^\ell\right)^k = \zeta^{k \cdot \ell} = \left(\zeta^k\right)^\ell = \tau(\sigma(\zeta)) = (\tau \circ \sigma)(\zeta).$$

By Theorem 11.4, this means that $\sigma \circ \tau = \tau \circ \sigma$ on all of $\mathbb{Q}(\zeta)$. Since σ, τ are two arbitrary elements, $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\zeta)$ is an abelian group.

Comment: Since $\sigma(\zeta) = \zeta^k$ and $\tau(\zeta) = \zeta^\ell$ must also be primitive nth roots of one when σ and τ are automorphisms of $\mathbb{Q}(\zeta)$, the possible values for ℓ and k here are the elements of the set $\{1, 2, \ldots, n\}$ that are *relatively prime* to n. This observation shows that $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\zeta) \simeq \mathbb{Z}_n^*$, the multiplicative group of units in the ring $\mathbb{Z}_n$, which is of course an abelian group.

Section 11.2

7b. The Galois correspondence here is the correspondence between subgroups of the Galois group and subfields of $\mathbb{Q}(\sqrt{2}, i)$ containing $\mathbb{Q}$. From Exercise 11 in Section 11.1 above, we have $G = \mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, i) = \{\mathrm{id}, \alpha, \beta, \gamma\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Since each non-identity element of G has order 2, there are exactly 5 subgroups of G, including the trivial subgroups $\{\mathrm{id}\}$ and G itself. The following diagram gives the inclusions between these subgroups (with the direction of the arrows indicating the direction of inclusion):



Now we show the fixed fields of each of these subgroups in a parallel diagram. For each subgroup H above, the subfield in the corresponding location is the fixed field

$$E_H = \{u \in \mathbb{Q}(\sqrt{2}, i) : \sigma(u) = u \text{ for all } \sigma \text{ in } H\ \}.$$

For instance, if $H = \{\mathrm{id}, \alpha\}$, then by definition, $u = u_0 + u_1\sqrt{2} + u_2 i + u_3 i\sqrt{2}$ $(u_i \in \mathbb{Q})$ is in E_H if and only if $\alpha(u) = u_0 - u_1\sqrt{2} + u_2 i - u_3 i\sqrt{2} = u$. This implies $u_1 = u_3 = 0$ and u_0, u_2 are arbitrary. Therefore

$$E_H = \{u_0 + u_2 i : u_0, u_2 \in \mathbb{Q}\} = \mathbb{Q}(i).$$

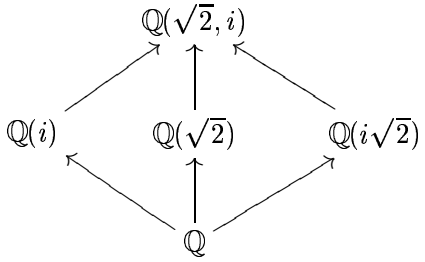
Similarly, if $H = \{\mathrm{id}, \beta\}$, then by definition, $u = u_0 + u_1\sqrt{2} + u_2 i + u_3 i\sqrt{2}$ $(u_i \in \mathbb{Q})$ is in E_H if and only if $\beta(u) = u_0 + u_1\sqrt{2} - u_2 i - u_3 i\sqrt{2} = u$. This implies $u_2 = u_3 = 0$ and u_0, u_1 are arbitrary. Therefore

$$E_H = \{u_0 + u_1\sqrt{2} : u_0, u_1 \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2})$$

in this case. Finally if $H = \{\mathrm{id}, \gamma = \alpha \circ \beta\}$, then by definition, $u = u_0 + u_1\sqrt{2} + u_2 i + u_3 i\sqrt{2}$ ($u_i \in \mathbb{Q}$) is in E_H if and only if $\gamma(u) = u_0 - u_1\sqrt{2} - u_2 i + u_3 i\sqrt{2} = u$. This implies $u_1 = u_2 = 0$ and u_0, u_3 are arbitrary. Therefore

$$E_H = \{u_0 + u_3 i\sqrt{2} : u_0, u_3 \in \mathbb{Q}\} = \mathbb{Q}(i\sqrt{2}).$$

Every element of $\mathbb{Q}(\sqrt{2}, i)$ is fixed by the identity subgroup. The only elements of $\mathbb{Q}(\sqrt{2}, i)$ fixed by *all* elements of G are the rational numbers. Hence we obtain the corresponding diagram of fixed fields and inclusions:



(Note that the arrows are all reversed from the first diagram!)