Mathematics 352 – Abstract Algebra II
Solutions for Problem Set 9
April 7, 2008

Section 11.2

8. First, $\mathrm{Gal}_E K$ is a subgroup of the abelian group $\mathrm{Gal}_F K$, so it is an abelian group. Second, since E is normal over F, by Theorem 11.11 (the Fundamental Theorem of Galois Theory), we have

$$\mathrm{Gal}_F E \simeq \mathrm{Gal}_F K/\mathrm{Gal}_E K.$$

Any time G is an abelian group and H is a normal subgroup, the quotient group G/H is abelian. (Proof: For all $a, b \in G$,

$$\begin{aligned} (Ha)(Hb) &= H(ab) \quad \text{(definition of coset product)} \\ &= H(ba) \quad \text{(since } ab = ba \text{ in } G\text{)} \\ &= (Hb)(Ha).) \end{aligned}$$

Therefore, $\mathrm{Gal}_F E$ is also abelian.

9. (a) By the result of Exercise 8, we know that $\mathrm{Gal}_E K$ and $\mathrm{Gal}_F E$ are both abelian. Now, we use some standard facts about cyclic groups. First, every subgroup of a cyclic group is cyclic (see Theorem 7.16 in Hungerford, or your text from Algebraic Structures). Then every quotient group G/H of a cyclic group is cyclic. This follows since if a is a generator of G, then every $b \in G$ satisfies $b = a^k$ for some $k \in \mathbb{Z}$. But then $Hb = Ha^k = (Ha)^k$, which shows that G/H is cyclic, generated by Ha.

(b) Since we assume K is Galois over F, the Galois correspondence is a one-to-one correspondence by Theorem 11.11. In the cyclic group $G = \mathrm{Gal}_F K \simeq \mathbb{Z}_n$, there is exactly one subgroup of order d for each divisor d of n. (If a generates G, then this subgroup is generated by $a^{n/d}$; see Exercise 40 in Section 7.3 of Hungerford.) Hence there is one intermediate field for each divisor d of n, and these are the only intermediate fields.

11. (a) The roots of $x^4 - 2 = 0$ are

$$x = \sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}.$$

Hence the splitting field over $\mathbb{Q}$ is

$$K = \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}).$$

We claim that $K = \mathbb{Q}(\sqrt[4]{2}, i)$. First, it is clear that $K \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$, since all the roots of $x^4 - 2 = 0$ are contained in this field. On the other hand $\mathbb{Q}(\sqrt[4]{2}, i) \subseteq K$ since $\sqrt[4]{2} \in K$ and $i = \frac{i\sqrt[4]{2}}{\sqrt[4]{2}} \in K$. Therefore the splitting field is equal to $\mathbb{Q}(\sqrt[4]{2}, i)$.

(b) From the tower of field extensions

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i),$$

we see that

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

The second factor on the right is 4 by Theorem 10.7, since the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ is the irreducible polynomial $x^4 - 2 \in \mathbb{Q}[x]$. The first factor on the right is 2 by Theorem 10.7, since the polynomial $x^2 + 1$ has i as a root and it is still irreducible in $\mathbb{Q}(\sqrt[4]{2})[x]$. (This follows since $x^2 + 1$ has no roots in $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$.) Hence $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$.

(c) Consider the extension $K/\mathbb{Q}(i)$. K is still the splitting field of $x^4 - 2$ over $\mathbb{Q}(i)$. The polynomial $x^4 - 2$ is still irreducible in $\mathbb{Q}(i)[x]$ since there are no roots in $\mathbb{Q}(i)$ and there are no polynomials of degree 2 with coefficients in $\mathbb{Q}(i)$ that divide $x^4 - 2$. (In other words there are no pairs r, s of roots of $x^4 - 2$ such that $(x - r)(x - s) \in \mathbb{Q}(i)[x]$. So by Theorem 11.3, there is a $\mathbb{Q}(i)$-automorphism σ of K that satisfies $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$. Since σ is a $\mathbb{Q}(i)$-automorphism, it satisfies $\sigma(i) = i$. But $\sigma(a) = a$ for all $a \in \mathbb{Q}$ as well, so σ defines an element of $\mathrm{Gal}_{\mathbb{Q}}K$.

(d) Using Corollary 11.13, the restriction of the complex conjugation mapping $a + ib \mapsto a - ib$ is also an element τ of $\mathrm{Gal}_{\mathbb{Q}}K$. Now by part (1) of Theorem 11.11, $|\mathrm{Gal}_{\mathbb{Q}}K| = [K : \mathbb{Q}] = 8$. Consider the action of the following combinations of σ and τ on the generators of K. We have

$$\begin{aligned}
\mathrm{id} : \sqrt[4]{2} &\mapsto \sqrt[4]{2} \\
i &\mapsto i \\
\sigma : \sqrt[4]{2} &\mapsto i\sqrt[4]{2} \\
i &\mapsto i \\
\sigma^2 : \sqrt[4]{2} &\mapsto -\sqrt[4]{2} \\
i &\mapsto i \\
\sigma^3 : \sqrt[4]{2} &\mapsto -i\sqrt[4]{2} \\
i &\mapsto i \\
\tau : \sqrt[4]{2} &\mapsto \sqrt[4]{2} \\
i &\mapsto -i \\
\sigma\tau : \sqrt[4]{2} &\mapsto i\sqrt[4]{2} \\
i &\mapsto -i \\
\sigma^2\tau : \sqrt[4]{2} &\mapsto -\sqrt[4]{2} \\
i &\mapsto -i \\
\sigma^3\tau : \sqrt[4]{2} &\mapsto -i\sqrt[4]{2} \\
i &\mapsto -i.
\end{aligned}$$

These give 8 distinct mappings on K by Theorem 11.4. Hence this shows

$$\mathrm{Gal}_{\mathbb{Q}}K = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}.$$

(e) We claim $\mathrm{Gal}_{\mathbb{Q}}K \simeq D_4$, the dihedral group of order 8. To see this note that the generators σ and τ satisfy $\sigma^4 = \mathrm{id}$, $\tau^2 = \mathrm{id}$ and

$$\begin{aligned}
\tau\sigma : \sqrt[4]{2} &\mapsto -i\sqrt[4]{2} \\
i &\mapsto -i.
\end{aligned}$$

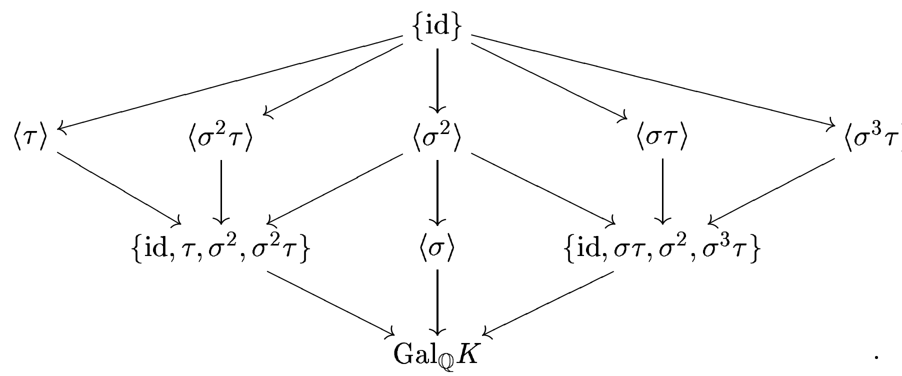
Hence $\tau\sigma = \sigma^3\tau = \sigma^{-1}\tau$. This shows that the generators satisfy the same relations as the generators of D_4, and both groups have order 8. It follows that $\mathrm{Gal}_{\mathbb{Q}}K \simeq D_4$. (Another way to say this is that, viewing D_4 as the group of symmetries of the square in $\mathbb{R}^2$, the mapping

$$\begin{array}{rcll} \varphi : \mathrm{Gal}_{\mathbb{Q}}K & \to & D_4 & \\ \sigma & \mapsto & r_1 & (\text{the } \frac{\pi}{2} \text{ rotation}) \\ \tau & \mapsto & v & (\text{one of the reflections}) \end{array}$$

is an isomorphism of groups – it is a one-to-one and onto group homomorphism.)

12. By Theorem 11.11, $\mathrm{Gal}_{\mathbb{Q}(i)}K$ is the subgroup of $\mathrm{Gal}_{\mathbb{Q}}K$ fixing all elements of $\mathbb{Q}(i)$. By examining the list in 11 (d), we see that this subgroup is $H = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3\}$, which is cyclic of order 4. The other four elements map i to $-i$ so they are not elements of $\mathrm{Gal}_{\mathbb{Q}(i)}K$. Therefore $\mathrm{Gal}_{\mathbb{Q}(i)}K \simeq \mathbb{Z}_4$.

13. The Galois correspondence is given by the following diagrams of subgroups and intermediate fields. D_4 contains 5 elements of order 2, so there are 5 subgroups of order 2. There are also 3 subgroups of order 4, one cyclic (namely, $\langle\sigma\rangle$), and the other two isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Here are the subgroups, with arrows showing the inclusions:



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

$$E_H = \{u \in \mathbb{Q}(\sqrt[4]{2}, i) : \alpha(u) = u \text{ for all } \alpha \text{ in } H\}.$$

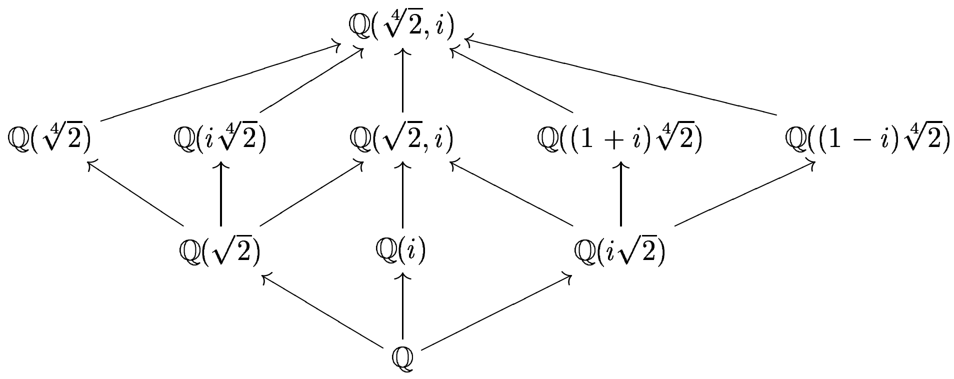
For instance, the fixed field of the subgroup $\langle\sigma\tau\rangle$ would be determined like this: If $a = a_0 + a_1\sqrt[4]{2} + a_2\sqrt{2} + a_3\sqrt[4]{8} + a_4 i + a_5 i\sqrt[4]{2} + a_6 i\sqrt{2} + a_7 i\sqrt[4]{8}$, satisfies $\sigma(\tau(a)) = a$, then $a_5 = a_1$, $a_2 = 0$, $a_3 = -a_7$, and $a_4 = 0$. a_0, a_6, a_1, a_3 are arbitrary and the general element of the fixed field looks like

$$a_0 + a_1(1+i)\sqrt[4]{2} + a_6 i\sqrt{2} + a_3(1-i)\sqrt[4]{8}.$$

We claim this is a general element of the field $\mathbb{Q}((1+i)\sqrt[4]{2})$. To see this note that if we write $\beta = (1+i)\sqrt[4]{2}$, then

$$\begin{array}{rcl} \beta^2 & = & -2i\sqrt{2} \\ \beta^3 & = & 2(1-i)\sqrt[4]{8} \\ \beta^4 & = & -8 \in \mathbb{Q}. \end{array}$$

This shows that the fixed field of $H = \langle\tau\rangle$ is $E_H = \mathbb{Q}((1-i)\sqrt[4]{2})$ as claimed. We also see that $\mathbb{Q}(i\sqrt{2})$ will be contained in $\mathbb{Q}(\beta)$ and $\mathbb{Q}(\gamma) = \mathbb{Q}((1-i)\sqrt[4]{2})$ from this computation. (Note that β^2 and γ^2 are rational multiples of $i\sqrt{2}$.) That is the fixed field of the subgroup $H = \{\mathrm{id}, \sigma\tau, \sigma^2, \sigma^3\tau\}$.



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