Modern Algebra 2 – MA 542 – Fall 2019 – R. Pollack
HW #9 Solutions

Section 48:
2). Since $\operatorname{irr}(\sqrt{2}, \mathbb{R}) = x - \sqrt{2}$ we have that $\sqrt{2}$ is the only conjugate of $\sqrt{2}$ over $\mathbb{R}$.

4) The conjugates of $\sqrt{2} - \sqrt{3}$ over $\mathbb{Q}$ are $\pm\sqrt{2} \pm \sqrt{3}$.

8) Let $\alpha = \sqrt{1+\sqrt{2}}$. Then $\alpha^2 = 1 + \sqrt{2}$ and thus α satisfies $x^2 - 1 - \sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$. We should check that this polynomial is irreducible over $\mathbb{Q}(\sqrt{2})$. To this end, assume that it has a root $a + b\sqrt{2}$. Then

$$(a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2} = 1 + \sqrt{2}$$

and thus

$$a^2 + 2b^2 = 1 \text{ and } 2ab = 1.$$

Combining these equations gives

$$a^2 + 2(1/2a)^2 = 1 \implies 4a^4 + 2 = 4a^2 \implies 2a^4 - 2a^2 + 1 = 0.$$

But this equation has no roots in $\mathbb{R}$ much less $\mathbb{Q}$. Thus $x^2 - 1 - \sqrt{2}$ is irreducible over $\mathbb{Q}(\sqrt{2})$ and the conjugates of α are $\pm\alpha$.

10) $\tau_2(\sqrt{2} + \sqrt{5}) = -\sqrt{2} + \sqrt{5}$.

12)

$$(\tau_5\tau_3)\left(\frac{\sqrt{2} - 3\sqrt{5}}{2\sqrt{3} - \sqrt{2}}\right) = \tau_5\left(\frac{\sqrt{2} - 3\sqrt{5}}{-2\sqrt{3} - \sqrt{2}}\right) = \frac{\sqrt{2} + 3\sqrt{5}}{-2\sqrt{3} - \sqrt{2}}$$

14)

$$\tau_3\left(\tau_5(\sqrt{2} - \sqrt{3} + (\tau_2\tau_5)(\sqrt{30}))\right) = \tau_3\left(\tau_5(\sqrt{2} - \sqrt{3} + \sqrt{30})\right) = \tau_3\left(\sqrt{2} - \sqrt{3} - \sqrt{30}\right) = \sqrt{2} + \sqrt{3} + \sqrt{30}$$

16) The fixed field of τ_3 is $\mathbb{Q}(\sqrt{2}, \sqrt{5})$. Indeed

$\tau_3(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{5}+e\sqrt{6}+f\sqrt{10}+g\sqrt{15}+h\sqrt{30}) = a+b\sqrt{2}-c\sqrt{3}+d\sqrt{5}-e\sqrt{6}+f\sqrt{10}-g\sqrt{15}-h\sqrt{30})$

iff $c = e = g = h = 0$ iff

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{5} + e\sqrt{6} + f\sqrt{10} + g\sqrt{15} + h\sqrt{30} = a + b\sqrt{2} + d\sqrt{5} + f\sqrt{10} \in \mathbb{Q}(\sqrt{2}, \sqrt{5}).$$

18). The fixed field of $\{\tau_2, \tau_3\}$ is $\mathbb{Q}(\sqrt{5})$. Indeed, for $\alpha = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{5}+e\sqrt{6}+f\sqrt{10}+g\sqrt{15}+h\sqrt{30}$, we have $\tau_2(\alpha) = \alpha$ iff $b = e = f = h = 0$ and $\tau_3(\alpha) = \alpha$ iff $c = e = g = h = 0$. Thus both τ_2 and τ_3 fix α iff $\alpha = a + d\sqrt{5} \in \mathbb{Q}(\sqrt{5})$.

22a) Since τ_2 fixes $\sqrt{3}$ and $\sqrt{5}$, clearly τ_2^2 also fixes these elements. Further, $\tau_2^2(\sqrt{2}) = -\tau_2(\sqrt{2}) = -(-\sqrt{2}) = \sqrt{2}$. Thus, τ^2 fixes all of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and is thus the identity element. This means τ_2 has order 2 (as it is not the identity itself). The same argument works for τ_3 and τ_5.

For (b), these 3 elements generate a group of size 8 with elements

$$\{1, \tau_2, \tau_3, \tau_5, \tau_2\tau_3, \tau_2\tau_5, \tau_3\tau_5, \tau_2\tau_3\tau_5\}.$$

The multiplication table is too hard for me to tex up right now. But it obeys the rules $\tau_2^2 = \tau_3^2 = \tau_5^2 = 1$ and τ_2, τ_3 and τ_5 all commute with one another.

34) If α is a root of $\operatorname{irr}(\alpha, F) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, then

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

with $a_i \in F$. Thus

$$\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_1\sigma(\alpha) + a_0 = 0$$

as σ is a homomorphism that fixes F. Hence, $\sigma(\alpha)$ is also a root of $\operatorname{irr}(\alpha, F)$.

If S is the set of roots of $\operatorname{irr}(\alpha, F)$, we have shown that σ induces a map from S to itself S. Further, since σ is invertible, σ^{-1} inverses the inverse map which forces σ to act as a permutation on S.

36a) As $\zeta^p = 1$ and $\zeta \neq 1$, we know that ζ has multiplicative order p. Thus $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ are all distinct and different from 1. Further, we have ζ^i is a root of $x^p - 1$ as $(\zeta^i)^p = (\zeta^p)^i = 1^i = 1$. If $i < p$, then $\zeta^i \neq 1$, and thus ζ^i is a root of $\frac{x^p-1}{x-1}$ as desired.

For part (b), fix an i such that $1 \leq i \leq p - 1$. Then there is a field homomorphism

$$\mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta^i)$$

which sends ζ to ζ^i and fixes $\mathbb{Q}$ as ζ and ζ^i are conjugate (as proven in class on Monday April 8th or see Corollary 48.5). But $\mathbb{Q}(\zeta^i) = \mathbb{Q}(\zeta)$. To see this note that $\zeta^i \in \mathbb{Q}(\zeta)$ and thus $\mathbb{Q}(\zeta^i) \subseteq \mathbb{Q}(\zeta)$. To see the reverse inclusion, let $y \in \mathbb{Z}$ denote a multiplicative inverse of i mod p so that $iy \equiv 1 \pmod{p}$. That is there is some x such that $iy + xp = 1$. Thus

$$(\zeta^i)^y = \zeta^{iy} = \zeta^{1-xp} = \zeta \cdot \zeta^{-xp} = \zeta \cdot (\zeta^p)^{-x} = \zeta \cdot 1^{-x} = \zeta.$$

This proves that $\zeta \in \mathbb{Q}(\zeta^i)$ and thus $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\zeta^i)$.

We thus have a map

$$\mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta^i) = \mathbb{Q}(\zeta)$$

which fixes $\mathbb{Q}$ and sends ζ to ζ^i. This is an automophism of $\mathbb{Q}(\zeta)$ which we will call σ_i.

Note that any automorphism $\tau \in \operatorname{Aut}(\mathbb{Q}(\zeta))$ sends ζ to some ζ^i and thus $\tau = \sigma_i$ for that i. Thus to prove that $\operatorname{Aut}(\mathbb{Q}(\zeta))$ is abelian we need to check $\sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i$ for all i, j. To see this, note that $\sigma_i \circ \sigma_j$ and $\sigma_j \circ \sigma_i$ both agree on $\mathbb{Q}$ as they both fix $\mathbb{Q}$. We thus only need to check that they agree on ζ. We have

$$(\sigma_i \circ \sigma_j)(\zeta) = \sigma_i(\zeta^j) = (\zeta^j)^i = \zeta^{ij}$$

and

$$(\sigma_j \circ \sigma_i)(\zeta) = \sigma_j(\zeta^i) = (\zeta^i)^j = \zeta^{ij}$$

as desired.

39a) Let $\varphi \in \mathrm{Aut}(E)$ and let x be a square of E. So $x = y^2$ for some $y \in E$. Then $\varphi(x) = \varphi(y^2) = \varphi(y)^2$. Thus $\varphi(x)$ is a square in E.
b) The fact that automorphisms of $\mathbb{R}$ take positive numbers to positive numbers is immediate from (a) as the positive numbers are exactly the squares of $\mathbb{R}$ with the exception of 0. But any automorphism always takes 0 to 0.
c) Let $\sigma \in \mathrm{Aut}(\mathbb{R})$. If $a < b$, then $b - a$ is positive. Hence by (b) $\sigma(b-a)$ is positive. This implies $\sigma(b) - \sigma(a)$ is positive and thus $\sigma(b) > \sigma(a)$.
d) Take $x \in \mathbb{R}$ and assume that $\sigma(x) \neq x$. If $\varphi(x) > x$, then there is some rational number r such that $\sigma(x) > r > x$. But then by (c) we have $\sigma(r) > \sigma(x)$. However, any automorphism always fixes $\mathbb{Q}$ and thus $\sigma(r) = r$. We deduce then that $r > \sigma(x)$. But this is a contradiction as $\sigma(x) > r > x$. The case $\sigma(x) < x$ works exactly the same and thus $\sigma(x) = x$.