Algebra II, Spring 2017

Solutions to Problem Set 2

1. Note that $gh(i) = -i$ and $gh(\rho) = g(i\rho) = -i\rho$, so $gh(i\rho) = -\rho$ and

$$gh(i\rho - \rho) = -\rho + i\rho.$$

So $i\rho - \rho$ is fixed by gh. Let $\alpha = i\rho - \rho$. We claim that the fixed field of the subgroup $\{e, gh\}$ is $\mathbf{Q}(\alpha)$. To show this, it is enough to show the degree of $\mathbf{Q}(\alpha)/\mathbf{Q}$ is 4. This follows if we show α is not the root of a polynomial of degree 2 in $\mathbf{Q}[x]$. But if $f(x) \in \mathbf{Q}[x]$ is the minimal polynomial of α, then the complex conjugate of α, $\bar{\alpha} = -i\rho - \rho$, should be a root of f as well. If $f(x)$ were of degree 2, then we would have $f(x) = (x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}$. But $\alpha + \bar{\alpha} = -2\rho \notin \mathbf{Q}$, so f has to have degree 4. So $\mathbf{Q}(\alpha)$ is the fixed field of $\{e, gh\}$. Similarly the fixed field of $\{e, gh^3\}$ is $\mathbf{Q}(i\rho + \rho)$.

If $H =< g, h^2 >= \{e, g, h^2, gh^2\}$, then $h(\rho) = i\rho$, so $h(\rho^2) = i\rho i\rho = -\rho^2$, so $h^2(\rho^2) = h(h(\rho^2)) = h(-\rho^2) = \rho^2$. Since ρ^2 is fixed by g too, ρ^2 is in E^H. The degree of $E^H/\mathbf{Q}$ is the index of H in G which is 2, and clearly $\mathbf{Q}(\rho^2)/\mathbf{Q} = \mathbf{Q}(\sqrt{2})/\mathbf{Q}$ is a degree 2 extension, so $E^H = \mathbf{Q}(\sqrt{2})$.

2. We have $\Delta^2 = -4a^3 - 27b^2$ for a cubic polynomial $x^3 + ax + b$.

(a) $x^3 + x^2 - 2x - 1 = (x + \frac{1}{3})^3 + (x + \frac{1}{3})(-\frac{7}{3}) - \frac{7}{27}$. So we look at the polynomial $y^3 - \frac{7}{3}y - \frac{7}{27}$. So $\delta^2 = 49$ and $\delta \in \mathbf{Q}$, so the Galois group is $\mathbf{Z}_3$.

(b) $\delta^2 = -2700$, and $\delta = 30\sqrt{3} \notin \mathbf{Q}(\sqrt{2}$, so the Galois group is S_3.

3. We prove by induction that if $\phi : F \simeq F'$ is a field isomorphism, $f(x) \in F[x]$ is an irreducible polynomial, $g = \phi(f) \in F'[x]$, E is the splitting field of $f(x)$, and E' is the splitting field of $g(x)$, then for every roots α of f and β of g there is an isomorphism $\psi : E \to E'$ extending ϕ and sending α to β. We use induction on $[E : F]$. If $[E : F] = 1$, there is nothing to prove. Assume $[E : F] = n$ and the statement is true when the degree of the extension is smaller than n. Let $m = \deg f = \deg g$. Then $F(\alpha) = \{c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1} | c_i \in F\}$ and $F'(\beta) = \{d_0 + d_1\beta + \cdots + d_{m-1}\beta^{m-1} | d_i \in F'\}$. It is easy to see that there is an isomorphism $\tilde{\phi} : F(\alpha) \to F'(\beta)$ sending

$c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1}$ to $\phi(c_0) + \phi(c_1)\beta + \cdots + \phi(c_{m-1})\beta^{m-1}$ (it is clear that this map is bijective and respects addition. to show it respects multiplication one can look at monomials of the form $c\alpha^i$.) Now since $E/F(\alpha)$ is also the splitting field of $f(x) \in F(\alpha)[x]$, the extension is Galois, so it is the splitting field of a polynomial $p(x)$. We set $q(x) = \tilde{\phi}(p)(x)$ and pick arbitrary roots of p and q. By induction hypothesis we can extend $\tilde{\phi}$ to an isomorphism $\psi : E \to E'$.

4. We proved this in class for $H_2 = G$. (in this case $E^{H_2} = E^G = F$.) The prove is exactly the same when H_2 is an arbitrary subgroup of G.

5. (a) If G is the group of permutations of $S = \{\alpha, -\alpha, \beta, -\beta\}$ such that $\sigma(-x) = -x$ for every $x \in S$, then G is isomorphic to D_8 (generated by an element of order 2: $\tau(\alpha) = -\alpha$ and $\tau(\beta) = -\beta$, and an element of order 4: $\rho(\alpha) = -\beta, \rho(\beta) = -\alpha$.) So $G = \{e, \tau, \rho, \rho^2, \rho^3, \tau\rho, \tau\rho^2, \tau\rho^3\}$ with $\rho^4 = e, \tau^2 = e$, and $\tau\rho = \rho^{-1}\tau$. Therefore G is isomorphic to D_8. Clearly Gal(E/$\mathbf{Q}$) is a subgroup of G. It can't be of order 2, since the minimal polynomial of every root has degree 4. The subgroups of order 4 or 8 in D_8 are isomorphic to $\mathbf{Z}_4, \mathbf{Z}_2 \times \mathbf{Z}_2$ or D_8.

(b) If $\alpha\beta = c \in \mathbf{Q}$, then for every $\sigma \in$ Gal(E/$\mathbf{Q}$), $\sigma(\alpha\beta) = \alpha\beta$. So $\sigma(\beta) = \frac{\alpha\beta}{\sigma(\alpha)}$. Therefore σ is determined by the image of α and since there are at most 4 such possibilities for the image of α, $|\text{Gal(E/}\mathbf{Q})| \leq 4$, and hence $|\text{Gal(E/}\mathbf{Q})| = 4$ by part (a). If $\sigma(\alpha) = \alpha$, then $\sigma = id$. If $\sigma(\alpha) = -\alpha$, then $\sigma^2 = id$. If $\sigma(\alpha) = \beta$, then $\sigma(\beta) = \alpha$, and therefore $\sigma^2 = id$. Similarly if $\sigma(\alpha) = -\beta$, $\sigma^2 = id$, so $G = \mathbf{Z}_2 \times \mathbf{Z}_2$.

(c) Let $c = \frac{\alpha}{\beta} - \frac{\beta}{\alpha} \in \mathbf{Q}$. Then $\sigma(c) = c$ for very $\sigma \in$ Gal(E/$\mathbf{Q}$). So again the image of β is determined by the image of α and therefore there are 4 possibilities for σ and $|\text{Gal(E/}\mathbf{Q})| = 4$. If $\sigma(\alpha) = -\beta$, then $\sigma(\beta)$ has to be $-\alpha$ in order for c to be fixed, and it is easy to see in this case σ has order 4, so the Galois group is $\mathbf{Z}_4$. Conversely if the Galois group if $\mathbf{Z}_4$, then since the only subgroup of D_8 which is isomorphic to $\mathbf{Z}_4$ is $\{e, \rho, \rho^2, \rho^3\}$, and ρ fixes c, every element of the Galois group fixes c, so $c \in \mathbf{Q}$.

6. Let $f(x) \in \mathbf{Q}[x]$ be an irreducible degree 3 polynomial, and let E be the splitting field of $f(x)$. Then $f(x)$ has at least one real root α and $\mathbf{Q}(\alpha) \subset E$. (every polynomial of odd degree over $\mathbf{R}[x]$ has at least one real root.) Since $f(x)$ is irreducible in $\mathbf{Q}[x]$, $\alpha \notin \mathbf{Q}$, so $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 3$. Since Gal(E/$\mathbf{Q}$) $= \mathbf{Z}_3$, $[E : \mathbf{Q}] = 3$, so $E = \mathbf{Q}(\alpha)$. Therefore, the other roots of f are generated by a real number over $\mathbf{Q}$ and are therefore real.