Math 306, Spring 2012
Homework 9 Solutions

(1) (10 pts) Let p be prime. Prove that the Galois group of $x^p - 2 \in \mathbb{Q}[x]$ is isomorphic to the group

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a, b \in \mathbb{Z}_p \text{ and } a \neq 0 \right\}.$$

(Hint: Let $\sigma_{k,\ell}$ be determined by $\sqrt[p]{2} \mapsto \sqrt[p]{2}\,\omega^k$ and $\omega \mapsto \omega^\ell$, where $\omega^p = 1$, and prove that $\sigma_{k,\ell} \circ \sigma_{m,n} = \sigma_{k+\ell m,\ell n}$.)

Solution: Each element of the Galois group is given by $\sigma_{k,\ell}$, determined by $\sqrt[p]{2} \mapsto \sqrt[p]{2}\,\omega^k$ and $\omega \mapsto \omega^\ell$, where $\omega^p = 1$. Here $k \in \mathbb{Z}_p$ and $\ell \in \mathbb{Z}_p^\times$. Let $\sigma_{k,\ell}, \sigma_{m,n}$ be two elements of the Galois group. Then $\sigma_{k,\ell} \circ \sigma_{m,n}(\sqrt[p]{2}\,\omega^k) = \sqrt[p]{2}\,\omega^{k+\ell m}$ and $\sigma_{k,\ell} \circ \sigma_{m,n}(\omega) = \omega^{\ell n}$. Hence $\sigma_{k,\ell} \circ \sigma_{m,n} = \sigma_{k+\ell m,\ell n}$. Let H be the Galois group of $x^p - 2$ over $\mathbb{Q}$. We define a map $\phi\colon H \to G$ given by

$$\phi(\sigma_{k,\ell}) = \begin{bmatrix} \ell & k \\ 0 & 1 \end{bmatrix}$$

for all $\sigma_{k,\ell} \in H$. This map is certainly well-defined and bijective. Let $\sigma_{k,\ell}, \sigma_{m,n} \in H$. Then

$$\phi(\sigma_{k,\ell} \circ \sigma_{m,n}) = \phi(\sigma_{k+\ell m,\ell n}) = \begin{bmatrix} \ell n & k + \ell m \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \ell & k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} n & m \\ 0 & 1 \end{bmatrix} = \phi(\sigma_{k,\ell})\phi(\sigma_{m,n}).$$

Hence ϕ is an isomorphism.

(2) (4 pts/part)
- (a) Let $f \in \mathbb{R}[x]$. Suppose that $z \in \mathbb{C}$ is a root of f. Prove that $\overline{z}$ (complex conjugate of z) is also a root of f.
- (b) Suppose that $f \in \mathbb{Q}[x]$ has degree 3. Use (a) to prove that, if the Galois group of f is isomorphic to $\mathbb{Z}_3$, then f has only real roots. (Hint: Prove the contrapositive, noticing that the conjugation automorphism has order 2.)

Solution:
- (a) Suppose that z is a root of the polynomial $f = c_0 + c_1 x + \cdots + c_n x^n \in \mathbb{R}[x]$. Then $c_0 + c_1 z + \cdots + c_n z^n = 0$. Take the complex conjugate of both sides, noting that $\overline{c_i} = c_i$ for all i. Then $c_0 + c_1 \overline{z} + \cdots + c_n \overline{z}^n = 0$ since conjugation is an $\mathbb{R}$-automorphism. Therefore $\overline{z}$ is a root of f.
- (b) Suppose that f does not have 3 real roots. Then f must have two complex roots and one real root. Hence the Galois group of f must contain complex conjugation, which is an element of order 2. Therefore the Galois group cannot be $\mathbb{Z}_3$, a contradiction.

(3) (4 pts/part) Consider the polynomial $f = x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$. Recall that we say that an extension $L\colon K$ is *Galois* or that L is *Galois over* K if $L\colon K$ is a normal and separable extension.
- (a) Prove that f is irreducible and find the roots of f.
- (b) Let α and β be roots of f that are not negatives of each other. Prove that $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ and $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{3})$. (Hint: Consider the degree $[\,\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta)\colon \mathbb{Q}(\sqrt{3})\,]$.)
- (c) Prove that $\mathbb{Q}(\alpha), \mathbb{Q}(\beta)$ and $\mathbb{Q}(\alpha, \beta)$ are all Galois over $\mathbb{Q}(\sqrt{3})$.
- (d) Prove that the Galois group of $\mathbb{Q}(\alpha, \beta)\colon \mathbb{Q}(\sqrt{3})$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.
- (e) Prove that the Galois group of $\mathbb{Q}(\alpha, \beta)\colon \mathbb{Q}$ is isomorphic to D_8 (recall that this is the dihedral group from 305; if you can't find it in your notes, look it up on Wikipedia). (Hint: Prove first that each σ in the Galois group is determined by its action on α and $\sqrt{2}\,i$.

Solution:
- (a) The polynomial is irreducible by Eisenstein with $p = 2$. By using the quadratic formula on x^2, we find that the roots of f are $\pm\sqrt{1 \pm \sqrt{3}}$.

(b) Let $\alpha = \sqrt{1+\sqrt{3}}$ and $\beta = \sqrt{1-\sqrt{3}}$. Certainly α is real but β is not, so $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$. Clearly $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta)$. Now we know that

$$[\,\mathbb{Q}(\beta)\colon \mathbb{Q}(\sqrt{3})\,] = [\,\mathbb{Q}(\beta)\colon \mathbb{Q}(\alpha)\cap\mathbb{Q}(\beta)\,][\,\mathbb{Q}(\alpha)\cap\mathbb{Q}(\beta)\colon \mathbb{Q}(\sqrt{3})\,].$$

Now $[\,\mathbb{Q}(\beta)\colon \mathbb{Q}(\sqrt{3})\,] = 2$ and $[\,\mathbb{Q}(\beta)\colon \mathbb{Q}(\alpha)\cap\mathbb{Q}(\beta)\,] > 1$, so it must then follow that

$$[\mathbb{Q}(\alpha)\cap\mathbb{Q}(\beta)\colon \mathbb{Q}(\sqrt{3})\,] = 1.$$

Hence $\mathbb{Q}(\alpha)\cap\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{3})$.

(c) Clearly all the extensions are separable. Since $\mathbb{Q}(\alpha)\colon \mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\beta)\colon \mathbb{Q}(\sqrt{3})$ both have degree 2, it follows that they are both normal extensions (this was a homework problem). Since $\mathbb{Q}(\alpha,\beta)$ is the splitting field of f over $\mathbb{Q}$, the extension $\mathbb{Q}(\alpha,\beta)\colon \mathbb{Q}$ is Galois. Hence $\mathbb{Q}(\alpha,\beta)\colon \mathbb{Q}(\sqrt{3})$ is Galois.

(d) If σ is a $\mathbb{Q}(\sqrt{3})$ automorphism of $\mathbb{Q}(\alpha,\beta)$, then let $c = \sigma(\alpha)$. Hence

$$c^2 = \sigma(\alpha^2) = \sigma(1+\sqrt{3}) = 1+\sqrt{3}.$$

So $c = \pm\alpha$. Notice also that $\alpha\beta = \sqrt{2}\,i$, so all $\mathbb{Q}(\sqrt{3})$-automorphisms are determined its behavior on α and $\sqrt{2}\,i$. The four such automorphisms are given by the following:

$$\begin{aligned}
\sigma_1\colon &\quad \alpha\mapsto\alpha, &&\quad \sqrt{2}\,i\mapsto\sqrt{2}\,i;\\
\sigma_2\colon &\quad \alpha\mapsto-\alpha, &&\quad \sqrt{2}\,i\mapsto\sqrt{2}\,i;\\
\sigma_3\colon &\quad \alpha\mapsto\alpha, &&\quad \sqrt{2}\,i\mapsto-\sqrt{2}\,i;\\
\sigma_4\colon &\quad \alpha\mapsto-\alpha, &&\quad \sqrt{2}\,i\mapsto-\sqrt{2}\,i.
\end{aligned}$$

All of these elements have order 1 or 2, so the Galois group is isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_2$.

(e) Every element of the Galois group is determined by its behavior on α and $\sqrt{2}\,i$. Note that α may be sent to $\pm\alpha$ or $\pm\beta$. The elements of the Galois group are as follows:

$$\begin{aligned}
\sigma_1\colon &\quad \alpha\mapsto\alpha, &&\quad \sqrt{2}\,i\mapsto\sqrt{2}\,i;\\
\sigma_2\colon &\quad \alpha\mapsto-\alpha, &&\quad \sqrt{2}\,i\mapsto\sqrt{2}\,i;\\
\sigma_3\colon &\quad \alpha\mapsto\beta, &&\quad \sqrt{2}\,i\mapsto\sqrt{2}\,i;\\
\sigma_4\colon &\quad \alpha\mapsto-\beta, &&\quad \sqrt{2}\,i\mapsto\sqrt{2}\,i;\\
\sigma_5\colon &\quad \alpha\mapsto\alpha, &&\quad \sqrt{2}\,i\mapsto-\sqrt{2}\,i;\\
\sigma_6\colon &\quad \alpha\mapsto-\alpha, &&\quad \sqrt{2}\,i\mapsto-\sqrt{2}\,i;\\
\sigma_7\colon &\quad \alpha\mapsto\beta, &&\quad \sqrt{2}\,i\mapsto-\sqrt{2}\,i;\\
\sigma_8\colon &\quad \alpha\mapsto-\beta, &&\quad \sqrt{2}\,i\mapsto-\sqrt{2}\,i.
\end{aligned}$$

Notice that σ_8 and σ_5 do not commute, so the Galois group is nonabelian. Also, we can compute that σ_7 and σ_8 are the only elements of order 4, so the Galois group must be D_8.

(4) (3 pts/part) Construct the subfield and subgroup lattice diagrams for extensions related to the following polynomials in $\mathbb{Q}[x]$. You may use any previous results about these polynomials.

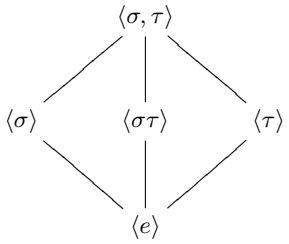
(a) $x^4 - 4x^2 + 2$

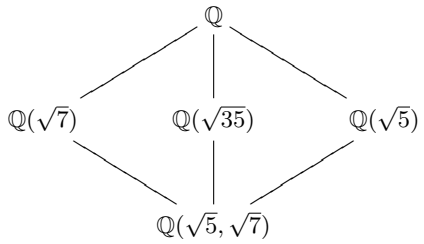
(b) $x^4 - 12x^2 + 35$

Solution:

(a) The roots are $\pm\sqrt{2\pm\sqrt{2}}$ and the Galois group is $\mathbb{Z}_4$. Let $\alpha = \sqrt{2+\sqrt{2}}$. Therefore the subgroup and subfield lattices are given as follows:

(b) The roots are $\pm\sqrt{7}$ and $\pm\sqrt{5}$. The Galois group is $\mathbb{Z}_2 \times \mathbb{Z}_2$ generated by σ and τ, where σ and τ are determined by $\sigma\colon \sqrt{5} \mapsto -\sqrt{5}$, $\sqrt{7} \mapsto \sqrt{7}$ and $\tau\colon \sqrt{5} \mapsto \sqrt{5}$, $\sqrt{7} \mapsto -\sqrt{7}$. Then we have the diagrams:





(5) (3 pts/part) Use the Fundamental Theorem of Galois Theory to prove the following. Let $L\colon K$ be a Galois extension with Galois group G.

(a) Suppose that M and N are intermediate fields with $M \subseteq N$. Prove that $N\colon M$ is normal iff N^* is normal in M^*.

(b) In this case, prove that the Galois group of $N\colon M$ is M^*/N^*.

(Hint: Each proof should be a maximum of two sentences long.)

Solution:

(a) Since $L\colon K$ is Galois, it follows that $L\colon M$ is Galois. Hence the Fundamental Theorem applied to $L\colon M$ states that, for any intermediate field N, we know that $N\colon M$ is normal iff N^* is normal in $\mathrm{Gal}(L/M) = M^*$.

(b) Again by the Fundamental Theorem, we have $\mathrm{Gal}(N/M) \cong \mathrm{Gal}(L/M)/\mathrm{Gal}(L/N) = M^*/N^*$.