Problem Set 12

Due Thursday, April 23

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, and our course notes.

I will post the .tex code for these problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly.* As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Please do not refer to theorems by their number in the course notes, as that can change.

Problem 1. Compute $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$.

Proof. Note that $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is the splitting field of the separable polynomial $(x^2-2)(x^2-3)$, so it is Galois. The degree is four as we have seen earlier, so the Galois group has four elements.

Any element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ must map $\sqrt{2}$ to another roots of x^2-2, so ± 2, and likewise must map $\sqrt{3}$ to $\pm\sqrt{3}$. Since $\sqrt{2},\sqrt{3}$ generate the field extension, the images of $\sqrt{2}$ and $\sqrt{3}$ determine the element of the Galois group. That is,

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) & \to & \{\pm\sqrt{2},\pm\sqrt{3}\} \\ \sigma & \mapsto & (\sigma(\sqrt{2}),\sigma(\sqrt{3})) \end{array}$$

is injective. By counting elements, this map must also be surjective. Thus, these determine the four elements:

$$\sigma_1\begin{bmatrix}\sqrt{2}\\ \sqrt{3}\end{bmatrix} = \begin{bmatrix}\sqrt{2}\\ \sqrt{3}\end{bmatrix},\ \sigma_2\begin{bmatrix}\sqrt{2}\\ \sqrt{3}\end{bmatrix} = \begin{bmatrix}-\sqrt{2}\\ \sqrt{3}\end{bmatrix},\ \sigma_3\begin{bmatrix}\sqrt{2}\\ \sqrt{3}\end{bmatrix} = \begin{bmatrix}\sqrt{2}\\ -\sqrt{3}\end{bmatrix},\ \sigma_4\begin{bmatrix}\sqrt{2}\\ \sqrt{3}\end{bmatrix} = \begin{bmatrix}-\sqrt{2}\\ -\sqrt{3}\end{bmatrix}.$$

Note that each element of the group squared (composed with itself twice) gives the identity map σ_1. The only group with four elements up to isomorphism with this property is $\mathbb{Z}/2\times\mathbb{Z}/2$. Thus, this is the Galois group. □

Problem 2. Let p be a prime number and let L be the splitting field of x^p-2 over $\mathbb{Q}$. In an earlier problem set, you showed that $L=\mathbb{Q}(b,\zeta)$ for $b=\sqrt[p]{2}$ and $\zeta=e^{2\pi i/p}$, and $[L:\mathbb{Q}]=p(p-1)$.

(a) Determine all the elements of $\mathrm{Gal}(L/\mathbb{Q})$.

We showed in an earlier problem set that $[L:\mathbb{Q}(b)]=p-1$, and ζ is a root of $x^{p-1}+\cdots+x+1$. Therefore, the minimum polynomial of ζ over $\mathbb{Q}(b)$ must be

$$m_{\zeta,\mathbb{Q}(b)} = x^{p-1}+\cdots+x+1.$$

Then $1,\zeta,\ldots,\zeta^{p-2}$ is a basis for L as a $\mathbb{Q}(b)$-vector space. Combining this with the basis for $\mathbb{Q}(b)/\mathbb{Q}$ above shows as in the proof of the Degree Formula that

$$B := \{b^m\zeta^j \mid 0\leqslant m\leqslant p-1, 0\leqslant j\leqslant p-2\}$$

is a basis for L as a vector space over $\mathbb{Q}$.

Let σ be any element of $G = \mathrm{Aut}(K/\mathbb{Q})$. Then by a theorem from class, $\sigma(b)$ must be another root of $x^p - 2$, so $\sigma(b) = b\zeta^{r_\sigma}$ for some $0 \leqslant r_\sigma \leqslant p-1$. Likewise, σ maps the root ζ of the polynomial $\Phi_p(x) = x^{p-1} + \cdots + 1 \in \mathbb{Q}[x]$ to another root $\sigma(\zeta) = \zeta^{s_\sigma}$ of Φ_p for some $1 \leqslant s_\sigma \leqslant p-1$. Hence for each element $b^m\zeta^j$ of the basis B above, we have

$$\sigma(b^m\zeta^j) = \sigma(b)^m\sigma(\zeta)^j = (b\zeta^{r_\sigma})^m(\zeta^{s_\sigma})^j = b^m\zeta^{mr_\sigma + js_\sigma}.$$

Since σ fixes $\mathbb{Q}$, then σ is a $\mathbb{Q}$-linear transformation, so the numbers $r_\sigma \in \{0, ..., p-1\}$ and $s_\sigma \in \{1, ..., p-1\}$ completely determine the automorphism σ of K.

Moreover, if $\sigma, \tau \in \mathrm{Aut}(K/\mathbb{Q})$ satisfy $r_\sigma = r_\tau$ and $s_\sigma = s_\tau$, then σ and τ fix both $\mathbb{Q}$ and have the same action on the basis B of $K/\mathbb{Q}$, so $\sigma = \tau$. Hence, there are at most $p(p-1)$ automorphisms of K/Q, each one associated to a pair of numbers $0 \leqslant r \leqslant p-1$ and $1 \leqslant s \leqslant p-1$.

Note that $x^p - 2$ is a polynomial of degree p with p distinct roots, so it is separable. Thus K is the splitting field of a separable polynomial over $\mathbb{Q}$, and thus $\mathbb{Q} \subseteq K$ is Galois. Therefore,

$$|G| = |\,\mathrm{Aut}(K/\mathbb{Q})| = [K : \mathbb{Q}] = p(p-1).$$

Hence for each $0 \leqslant r \leqslant p-1$ and $1 \leqslant s \leqslant p-1$ there is an automorphism $\tau_{r,s} : K \to K$ that fixes $\mathbb{Q}$ and satisfies

$$\tau_{r,s}(b^m\zeta^j) = b^m\zeta^{mr+js} \quad \text{for all} \quad b^m\zeta^j \in B.$$

Therefore,

$$\mathrm{Aut}(K/\mathbb{Q}) = \{\tau_{r,s} \mid 0 \leqslant r \leqslant p-1, 1 \leqslant s \leqslant p-1\}.$$

(b) Decide, with justification, whether $G = \mathrm{Gal}(L/\mathbb{Q})$ is abelian.

Proof. First, we have

$$\begin{aligned} \tau_{r,s} \circ \tau_{r',s'}(b^m\zeta^j) &= \tau_{r,s}(b^m\zeta^{mr'+js'}) \\ &= b^m\zeta^{mr+(mr'+js')s} \\ &= b^m\zeta^{mr+mr's+js's} \end{aligned}$$

and thus, interchanging the roles of r, s and r', s' we have

$$\tau_{r,s} \circ \tau_{r',s'}(b^m\zeta^j) = b^m\zeta^{mr'+mrs'+js's}.$$

This shows that

$$\begin{aligned} \tau_{r,s} \circ \tau_{r',s'} = \tau_{r,'s'} \circ \tau_{r,s} \quad &\iff \quad mr + mr's + js's \equiv mr' + mrs' + js's \pmod p \text{ for all } m, j \\ &\iff \quad m(r - r' + r's - rs') \equiv 0 \pmod p \text{ for all } 0 \leqslant m \leqslant p-1 \\ &\iff \quad r - r' + r's - rs' \equiv 0 \pmod p. \end{aligned}$$

If $p = 2$ then $s = s' = 1$ and the above shows that G is abelian. In fact, note that when $p = 2$ then $|\mathrm{Gal}(K/\mathbb{Q})| = 2$, and since there is only one group of order 2, we conclude that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2$ is abelian.

However, if $p > 2$, then taking for example $r = 0$, $r' = 1$, and $s = 2$ shows that that

$$\tau_{0,2} \circ \tau_{1,s'} \neq \tau_{1,s'} \circ \tau_{0,2},$$

since

$$1 \not\equiv 0 \pmod p.$$

Thus G is not abelian for $p > 2$. □

Problem 3. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible cubic (degree 3) polynomial having exactly one real root. Let L be the splitting field of $f(x)$ over $\mathbb{Q}$. Show that $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$.

Proof. Let a be the real root of f, and let b, c be the other two roots. Note that b and c are complex conjugates. In particular, a, b, and c are all distinct. Thus f is separable, and thus $\mathbb{Q} \subseteq L$ is Galois, so $|\operatorname{Aut}(L/\mathbb{Q})| = [L : \mathbb{Q}]$.

Since f has three distinct roots, $\mathrm{Gal}(L/\mathbb{Q})$ is a subgroup of S_3, and thus $|\mathrm{Gal}(L/\mathbb{Q})| \leqslant |S_3| = 6$. Since f is irreducible, it is the minimal polynomial of a, b, and c. In particular, $[L : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}] = 3$. Applying the Degree Formula to $\mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq L$, we conclude that $3|[L : \mathbb{Q}]$. Moreover, $b, c \notin \mathbb{R}$, so $b, c \notin \mathbb{Q}(a)$. In particular, $[L : \mathbb{Q}(a)] \geqslant 2$. Thus by the Degree Formula we have $[L : \mathbb{Q}] \geqslant 2 \cdot 3 = 6$, and we conclude that $[L : \mathbb{Q}] = 6$. The only subgroup of S_3 of order 6 is S_3, so $\operatorname{Aut}(L/\mathbb{Q}) \cong S_3$. □

Problem 4. Assume $F \subseteq L$ is a finite extension of fields and that the characteristic of F is p, where p is a prime. Suppose there exists an element $a \in L$ such that $a \notin F$ but $a^p \in F$.

(a) Prove $\sigma(a) = a$ for all $\sigma \in \operatorname{Aut}(L/F)$.

Proof. Let $a^p = b \in F$. Since a is a root of the polynomial $x^p - b$, all of whose coefficients are in F, we know $\sigma(a)$ must also be root of this polynomial. But, by the Freshman's Dream, $x^p - b$ factors as $(x - a)^b$ in $\overline{F}[x]$, and so this polynomial has just one root, which is a. So $\sigma(a) = a$. □

(b) Prove that $F \subseteq L$ is not Galois.

Proof. By part (a), every element of $\operatorname{Aut}(L/F)$ fixes a and thus also fixes $F(a)$. That is, $\operatorname{Aut}(L/F) = \operatorname{Aut}(L/F(a))$. Since $F \neq F(a)$, $[L : F(a)] < [L : F]$. Then

$$|\operatorname{Aut}(L/F)| = |\operatorname{Aut}(L/F(a))| \leqslant [L : F(a)] < [L : F].$$

In particular, $|\operatorname{Aut}(L/F)| < [L : F]$, so the extension is not Galois. □

Problem 5. Let p be a prime, and $n > 1$. Let $\mathbb{F}_p$ denote the field with p elements, and $\mathbb{F}_{p^n}$ denote the field with p^n elements. Show that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n$, and find a generator.

Proof. First we note that $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois, since we constructed it as the splitting field of the separable polynomial $x^{p^n} - x$.

We claim that the pth power map $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $F(a) = a^p$ generates the Galois group. Note first that this is a ring homomorphism by Freshman's Dream, and since it is injective (as fields are domains), it is also surjective. Thus, it is an automorphism.

Now, to see that it generates the Galois group, since the Galois group has n elements, it suffices to show that the order of F is at least n. Suppose otherwise; i.e., that $F^e = \mathrm{id}_{\mathbb{F}_{p^n}}$ for some $e < n$. Then $a^{p^e} = a$ for all $a \in \mathbb{F}_{p^n}$, so every element of $\mathbb{F}_{p^n}$ is a root of $x^{p^e} - x$. But this polynomial has degree p^e and thus has at most $p^e < p^n$ roots, a contradiction. Thus $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle F \rangle \cong \mathbb{Z}/n$. □