Math 114 Homework 5

(due Thursday, 6 March)

Michael Knopf

1. (Exercise 13 in DF §14.2.) Let $f(X) \in \mathbf{Q}[X]$ be a cubic, and let K be a splitting field for $f(X)$ over $\mathbf{Q}$. Prove that if $\operatorname{Aut} K/\mathbf{Q}$ is a cyclic group of order 3, then all the roots of $f(X)$ (in $\mathbf{C}$) are real.

Proof. We may assume that $K \subseteq \mathbb{C}$, since otherwise we could just take an embedding of K in $\mathbb{C}$. Suppose $\operatorname{Aut}(K/\mathbb{Q})$ is a cyclic group of order 3, and assume for a contradiction that $f(x)$ has a root $\alpha \in K$ that is not real. Since the automorphism of complex conjugation on $\mathbb{C}$ fixes the subfield $\mathbb{Q}$, we know that $\overline{\alpha}$ is another distinct root. Since $\operatorname{Aut}(K/\mathbb{Q}) \cong \mathbb{Z}_3$, all of its nontrivial elements must have order 3. However, $K \supset \mathbb{R}$ contains non-real elements, so complex conjugation is a nontrivial automorphism of K fixing $\mathbb{Q}$ with order 2, a contradiction.

□

2. (Adapted from Exercise 18 in DF §14.2.) Let K/F be a (finite) Galois extension with $[K : F] = n$. For each $\alpha \in K$, define the *trace* of α to be

$$Tr_{K/F}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha).$$

(a) Prove that $Tr_{K/F}(\alpha) \in F$ for any $\alpha \in K$.

Proof. Let $\tau \in \mathrm{Gal}(K/F)$. Then

$$\tau(Tr_{K/F}(\alpha)) = \tau\left(\sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha)\right) = \sum_{\sigma \in \mathrm{Gal}(K/F)} \tau \circ \sigma(\alpha) = \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha) = Tr_{K/F}(\alpha)$$

because τ acts as an permutation on $\mathrm{Gal}(K/F)$, so $\{\tau \circ \sigma : \sigma \in \mathrm{Gal}(K/F)\} = \mathrm{Gal}(K/F)$. Since $Tr_{K/F}(\alpha)$ is in the fixed field of an arbitrary $\tau \in \mathrm{Gal}(K/F)$, and we know the fixed field is F, $Tr_{K/F}(\alpha) \in F$. □

(b) Prove that $Tr_{K/F}(\alpha + \beta) = Tr_{K/F}(\alpha) + Tr_{K/F}(\beta)$ for any $\alpha, \beta \in K$.

Proof.

$$\begin{aligned} Tr_{K/F}(\alpha+\beta) &= \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha+\beta) = \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha) + \sigma(\beta) \\ &= \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha) + \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\beta) = Tr_{K/F}(\alpha) + Tr_{K/F}(\beta) \end{aligned}$$

□

(c) Suppose $K = F(\gamma)$ for some $\gamma \in K$ such that $\gamma^2 \in F$ and $\gamma \notin F$. Show that for any $a, b \in F$, $Tr_{K/F}(a + b\gamma) = 2a$.

Proof. K is the splitting field for the irreducible polynomial $x^2 - \gamma^2$, since it splits as $(x+\gamma)(x-\gamma)$ over K. Thus it is a Galois extension with Galois group $\{id, \sigma\}$, where σ is defined by $\gamma \mapsto -\gamma$. We know this is the full group because $\mathrm{Gal}(K/F)$ must have order $[K : F] = 2$, and σ is the only possible nontrivial automorphism. So

$$Tr_{K/F}(a + b\gamma) = id(a + b\gamma) + \sigma(a + b\gamma) = a + b\gamma + a - b\gamma = 2a$$

□

(d) Given $\alpha \in K$, let $m_\alpha(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_1 X + a_0 \in F[X]$ be the minimal polynomial for α over F. Prove that $Tr_{K/F}(\alpha) = -\frac{n}{d} a_{d-1}$.

Proof. Since K is Galois and $m_\alpha(x)$ is irreducible, m_α must be separable with d distinct roots $\alpha = \alpha_1, \ldots, \alpha_d$ in K. Let E be the splitting field for $m_\alpha(x)$ over F, so that $F \subset E \subset K$. Then E is also a Galois extension with Galois group H of order d, which is isomorphic to the quotient $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/H)$. Thus the cosets of $\mathrm{Gal}(K/H)$ in $\mathrm{Gal}(K/F)$ each have size n/d, and two automorphisms from $\mathrm{Gal}(K/F)$ have the same action on E if and only if they are in the same coset of $\mathrm{Gal}(K/H)$. Thus, for each root α_i, there are exactly n/d automorphisms in $\mathrm{Gal}(K/F)$ which map α to α_i. Therefore,

$$Tr_{K/F}(\alpha) = \frac{n}{d}(\alpha_1 + \cdots + \alpha_d).$$

Now, we know that $m_\alpha(x) = (x - \alpha_1)\cdots(x - \alpha_d)$. The ways to make terms containing a factor of degree $d-1$ are to take $-\alpha_i$ from one factor, and take x from every other factor when distributing. Thus $a_{d-1} = -\alpha_1 - \cdots - \alpha_d = -(\alpha_1 + \cdots + \alpha_d)$. So $Tr_{K/F}(\alpha) = -\frac{n}{d}a_{d-1}$. □

3. (Exercises 21 and 22 in DF §14.2.) Let K/F be a (finite) Galois extension, and let $\sigma \in \mathrm{Aut}\, K/F$ be any automorphism.

   (a) Use the linear independence of characters to show that there is an element $\alpha \in K$ with $Tr_{K/F}(\alpha) \neq 0$.

Proof. Suppose, for all $\alpha \in K$, that

$$Tr_{K/F}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha) = 0.$$

Then $\sigma_1, \ldots, \sigma_n$ are linearly dependent as functions, since this nontrivial linear combination of them is identically zero. This contradicts the linear independence of characters. □

   (b) Suppose that $\alpha \in K$ is of the form $\alpha = \frac{\beta}{\sigma(\beta)}$ for some nonzero $\beta \in K$. Prove that $N_{K/F}(\alpha) = 1$.

Proof. Again, σ acts on $\mathrm{Aut}\, K/F$ as a permutation. So

$$N_{K/F}(\sigma(\beta)) = \prod_{\tau \in \mathrm{Gal}\, K/F} \tau \circ \sigma(\beta) = \prod_{\tau \in \mathrm{Gal}\, K/F} \tau(\beta) = N_{K/F}(\beta).$$

Thus, $N_{K/F}(\alpha) = \dfrac{N_{K/F}(\beta)}{N_{K/F}(\sigma(\beta))} = \dfrac{N_{K/F}(\beta)}{N_{K/F}(\beta)} = 1$, since we have shown the norm is multiplicative. □

   (c) Suppose that $\alpha \in K$ is of the form $\alpha = \beta - \sigma(\beta)$ for some $\beta \in K$. Prove that $Tr_{K/F}(\alpha) = 0$.

Proof. Again, σ acts on $\mathrm{Aut}\, K/F$ as a permutation. So

$$Tr_{K/F}(\sigma(\beta)) = \sum_{\tau \in \mathrm{Gal}\, K/F} \tau \circ \sigma(\beta) = \sum_{\tau \in \mathrm{Gal}\, K/F} \tau(\beta) = Tr_{K/F}(\beta).$$

Thus, $Tr_{K/F}(\alpha) = Tr_{K/F}(\beta - \sigma(\beta)) = Tr_{K/F}(\beta) - Tr_{K/F}(\sigma(\beta)) = Tr_{K/F}(\beta) - Tr_{K/F}(\beta) = 0$, since the trace is additive. □

4. (Exercise 23 in DF §14.2.) Let K/F be a Galois extension with cyclic Galois group of order n generated by an automorphism σ. Suppose $\alpha \in K$ has $N_{K/F}(\alpha) = 1$. Prove that α is of the form $\alpha = \frac{\beta}{\sigma(\beta)}$ for some nonzero $\beta \in K$.

   [Hint: By the linear independence of characters show there exists some $\theta \in K$ such that the element

$$\beta = \theta + \alpha\sigma(\theta) + \alpha\sigma(\alpha)\sigma^2(\theta) + \ldots + \alpha\sigma(\alpha)\ldots\sigma^{n-2}(\alpha)\sigma^{n-1}(\theta)$$

is nonzero. Compute $\frac{\beta}{\sigma(\beta)}$ using the fact that $N_{K/F}(\alpha) = 1$.]

Proof. Since $\mathrm{Gal}\, K/F = \{\sigma^i : 0 \leq i < n\}$, linear independence of characters implies that there is some nonzero θ for which $\beta = \sigma^0(\theta) + \alpha\sigma(\theta) + \alpha\sigma(\alpha)\sigma^2(\theta) + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(\theta) \neq 0$, since the coefficients of each $\sigma^i(\theta)$ in this linear combination are scalars from the field K on which these characters take their values, and it cannot be $\theta = 0$, since otherwise this expression is 0.

Now, we have

$$\begin{aligned}\alpha\sigma(\beta) &= \alpha\sigma(\theta) + \alpha\sigma(\alpha)\sigma^2(\theta) + \alpha\sigma(\alpha)\sigma^2(\alpha)\sigma^3(\theta) + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha)\sigma^n(\theta) \\ &= \alpha\sigma(\theta) + \alpha\sigma(\alpha)\sigma^2(\theta) + \alpha\sigma(\alpha)\sigma^2(\alpha)\sigma^3(\theta) + \cdots + \theta \\ &= \beta\end{aligned}$$

because $N_{K/F}(\alpha) = \alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha) = 1$ and $\sigma^n(\theta) = \theta$, because σ has order n. Since β is nonzero, $\alpha = \dfrac{\beta}{\sigma(\beta)}$. □

5. (Exercise 25 in DF §14.2.) Let $D \in \mathbf{N}$ be a positive integer that is not the square of any integer. Determine all solutions $(a, b) \in \mathbf{Q}^2$ of the equation $a^2 + Db^2 = 1$.

   [Hint: see the hint to Exercise 24 in DF §14.2; use Exercise 17(c) (from HW04) together with Exercise 23 (above).]

Proof. Notice that $(a, b) \in \mathbb{Q}^2$ is a solution to the equation $a^2 + Db^2 = 1$ if and only if $N_{\mathbb{Q}(\sqrt{-D})/\mathbb{Q}}(a + b\sqrt{-D}) = a^2 + Db^2 = 1$.

$\mathbb{Q}(\sqrt{-D})$ is a Galois extension of degree 2, since the minimal polynomial of $\sqrt{-D}$ over $\mathbb{Q}$ is $x^2 + D$, which is separable and has both roots in this extension, thus $\mathbb{Q}(\sqrt{-D})$ is the splitting field for $x^2 + D$. So the Galois group of $\mathbb{Q}(\sqrt{-D})/Q$ is a cyclic group of order 2. The only possible nontrivial automorphism fixing $\mathbb{Q}$ is that determined by $\sqrt{-D} \mapsto -\sqrt{-D}$, since these are both roots of $x^2 + D$. This map is complex conjugation. So the Galois group consists just of the identity and complex conjugation.

By the previous exercise, all elements of norm 1 in $\mathbb{Q}(\sqrt{-D})$ are of the form $\dfrac{\beta}{\sigma(\beta)}$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{-D})/\mathbb{Q})$ and some nonzero $\beta \in \mathbb{Q}(\sqrt{-D})$. If σ is the identity, then this expression simply reduces to 1. So the only other elements of norm 1 are found when σ is complex conjugation. However, 1 can also be obtained by using complex conjugation if we just let $\beta = 1$, for instance. Therefore, *all* elements of norm 1 are of the form $\beta/\overline{\beta}$ for some $\beta \neq 0$.

Any nonzero $\beta \in \mathbb{Q}(\sqrt{-D})$ is of the form $\beta = s + t\sqrt{-D}$ for some $s, t \in \mathbb{Q}$, not both zero. So all elements of norm 1 are of the form

$$\frac{\beta}{\overline{\beta}} = \frac{\beta}{\overline{\beta}} \cdot \frac{\beta}{\beta} = \frac{\beta^2}{N(\beta)} = \frac{s^2 - t^2 + 2st\sqrt{-D}}{s^2 + Dt^2} = \frac{s^2 - t^2}{s^2 + Dt^2} + \frac{2st}{s^2 + Dt^2}\sqrt{-D}.$$

Therefore, all rational solutions to $a^2 + Db^2 = 1$ are of the form $(a, b) = \left(\dfrac{s^2 - t^2}{s^2 + Dt^2}, \dfrac{2st}{s^2 + Dt^2}\right)$. □

6. (Exercise 28 in DF §14.2.) Let F be a field, $f(X) \in F[X]$ an irreducible polynomial of degree n over F, L a splitting field of $f(X)$ over F, and $\alpha \in L$ a root of $f(X)$. If K is any Galois extension of F contained in L, show that the polynomial $f(X)$ splits into a product of m irreducible polynomials each of degree d over K, where $m = [F(\alpha) \cap K : F]$ and $d = [K(\alpha) : K]$.

   [Hint: If H is the subgroup of the Galois group of L over F corresponding to K, then the factors of $f(X)$ over K correspond to the orbits of H on the roots of $f(X)$. Then use Exercise 9 of DF §4.1 (which you may cite without proof).]

Proof. Let A be the set of roots of $f(x)$ in L, and consider the irreducible factors of $f(x)$ over K. Each of these has a corresponding set of roots, which is a subset of A. So let $\mathcal{O}_i$ be the set of roots of the ith irreducible factor of $f(x)$ over K.

Let $H = \mathrm{Gal}(L/K) \subseteq \mathrm{Gal}(L/F)$. $\mathrm{Gal}(L/F)$ acts transitively on A, since it must permute the roots of $f(x)$. However, H fixes the coefficients of each irreducible factor of $f(x)$ over K, thus it must permute the set $\mathcal{O}_i$ of roots of the ith factor, for each i. We know that the action of H on $\mathcal{O}_i$ is transitive, since a map that sends one root of this irreducible factor to another can always be extended to an automorphism on all of L. Thus the $\mathcal{O}_i$ are the orbits of H on A.

One of these factors has α as a root, and thus has degree d, since the degree d of $K(\alpha)$ over K is that of an irreducible polynomial over K with α as a root. So the orbit corresponding to this factor has d elements, which

$$
\begin{tikzcd}[arrows=dash]
 & L \arrow[dl] \arrow[ddr] & \\
K(\alpha) \arrow[dd, "d"'] & & \\
 & & F(\alpha) \arrow[ddl] \\
K \arrow[dr] & & \\
 & F(\alpha) \cap K \arrow[d, "m"] & \\
 & F &
\end{tikzcd}
$$

are the roots of this factor. L/K is a Galois extesions, so H is a normal subgroup of G. Thus, by exercise 9 in section 4.1, the orbits must all have the same number of elements. So each orbit contains d elements, meaning that each irreducible factor of $f(x)$ over K has degree d.

The Galois group of $L/F(\alpha)$ is the subgroup of automorphisms from $G = \text{Gal}(L/F)$ which fix $F(\alpha)$, meaning that they stabilize α. Thus $\text{Gal}(L/F(\alpha)) = G_\alpha$. By part 5 of the Galois correspondence theorem, the Galois group of $F(\alpha) \cap K$ is $< G_\alpha, H >= HG_\alpha$. Therefore, $m = [F(\alpha) \cap K : F] = |G : HG_\alpha|$, which by exercise 9 is the number of orbits of H on A. Since each orbit corresponds to a distinct irreducible factor of $f(x)$ over K, there must be exactly m such factors.

$\square$