Math 114 Homework 1
Michael Knopf
(due Thursday, 29 January)

1. (Exercise 7 in DF §13.2.) Prove that $\mathbf{Q}(\sqrt{2}+\sqrt{3}) = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. (One inclusion is obvious; for the other consider powers of $\sqrt{2}+\sqrt{3}$.) Find an irreducible polynomial $p(X) \in \mathbf{Q}[X]$ such that $p(\sqrt{2}+\sqrt{3}) = 0$.

Proof. All we need to show is that $\sqrt{2}+\sqrt{3} \in \mathbf{Q}(\sqrt{2}, \sqrt{3})$ and $\sqrt{2}, \sqrt{3} \in \mathbf{Q}(\sqrt{2}+\sqrt{3})$, since $\mathbf{Q}(A)$ is defined to be the intersection of all fields containing $\mathbf{Q}$ and A.

Clearly, $\mathbf{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbf{Q}(\sqrt{2}, \sqrt{3})$ because we can simply add $\sqrt{2}$ and $\sqrt{3}$ to obtain the primitive the primitive element of $\mathbf{Q}(\sqrt{2}+\sqrt{3})$.

To see that $\mathbf{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbf{Q}(\sqrt{2}+\sqrt{3})$, note that

$$\frac{1}{2}(\sqrt{2}+\sqrt{3})^3 - \frac{9}{2}(\sqrt{2}+\sqrt{3}) = \frac{1}{2}(11\sqrt{2}+9\sqrt{3}) - \frac{9}{2}(\sqrt{2}+\sqrt{3}) = \sqrt{2},$$

so $\sqrt{2} \in \mathbf{Q}(\sqrt{2}+\sqrt{3})$. Therefore, $\sqrt{3} = (\sqrt{2}+\sqrt{3}) - \sqrt{2} \in \mathbf{Q}(\sqrt{2}+\sqrt{3})$ as well.

An irreducible polynomial $p(X) \in \mathbf{Q}[X]$ such that $p(\sqrt{2}+\sqrt{3}) = 0$ is

$$p(X) = (X + (\sqrt{2}+\sqrt{3}))^2 (X - (\sqrt{2}+\sqrt{3}))^2 = X^4 - 10X^2 + 1.$$

The only factors of $p(X)$ we need to check for containment in $\mathbf{Q}[X]$ are

$$(X + (\sqrt{2}+\sqrt{3}))(X - (\sqrt{2}+\sqrt{3})) = X^2 - 5 - 2\sqrt{6} \notin \mathbf{Q}[X]$$

and

$$(X + (\sqrt{2}+\sqrt{3}))^2 = X^2 + 2(\sqrt{2}+\sqrt{3})X + 2\sqrt{6} + 5 \notin \mathbf{Q}[X]$$

thus $p(X)$ is indeed irreducible in $\mathbf{Q}[X]$ (the other non-unit factor is the conjugate of the $(X+(\sqrt{2}+\sqrt{3}))^2$, so it also contains non-rational coefficients).

□

2. (Exercise 12 in DF §13.2.) Suppose the degree of the extension K/F is a prime p. Show that any subfield E of K containing F is either K or F.

Proof. We will first show that if $A \subseteq B \subseteq C$ is a chain of subfields, then $[C : A] = [C : B][B : A]$.

Let $n = [C : B]$ and $m = [B : C]$. Let $v_1, \ldots, v_n$ be a basis for C over B and let $u_1, \ldots, u_m$ be a basis for B over A. We will show that $S = \{v_i u_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ forms a basis for C over A.

First, we need to show that S spans C over A. Let $v \in C$. Since $v_1, \ldots, v_n$ is a basis for C over B, there exist constants $b_1, \ldots, b_n \in B$ such that $v = b_1 v_1 + \cdots + b_n v_n$.

Since $u_1, \ldots, u_m$ is a basis for B over A, there exist constants $a_{i,j}$ such that $b_i = a_{i,1}u_1 + \cdots + a_{i,m}u_m$.

Therefore,

$$v = \sum_{i=1}^{n} b_i v_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_{i,j} u_j \right) v_i = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{i,j} u_j v_i.$$

The righthand side is a linear combination of elements of S with coefficients in A, thus S spans C over A.

Next, to see that S is linearly independent, suppose that

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{i,j} u_j v_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_{i,j} u_j \right) v_i = 0.$$

Since $v_1, \ldots, v_n$ are linearly independent over B and $\sum_{j=1}^m a_{i,j} u_j \in B$ for each i, we must have $\sum_{j=1}^m a_{i,j} u_j = 0$ for each i. Since $u_1, \ldots, u_m$ are linearly independent over A and $a_{i,j} \in A$ for each i, j, we must have $a_{i,j} = 0$ for each i, j. Therefore, S is linearly independent over A and has $n \cdot m$ elements, so $[A : C] = n \cdot m$.

Now, suppose that $[A : B] = 1$. Then 1 forms a basis for A over B, so $A = \{b \cdot 1 : b \in B\} = B$. It follows that if $[A : B] = [A : C]$ then $[B : C] = 1$, thus $B = C$.

Since $[K : F] = p$, if $F \subseteq E \subseteq K$ then either $[K : E] = p$ or $[K : E] = 1$, since $[K : E] \mid p$. Therefore, by the previous paragraph, either $E = K$ or $E = F$.

□

3. (Exercise 19 in DF §13.2.) Let K be an extension of F of degree $n \in \mathbf{N}$.

(a) For any $\alpha \in K$, prove that the map $K \to K$ given by $x \mapsto \alpha x$ is an F-linear transformation of K (i.e. a linear transformation of K as an F-vector space).

Proof. Let $x, y \in K$ and $c \in F$. Let T denote the map given above. Then

$$T(cx + y) = \alpha(cx + y) = \alpha cx + \alpha y = c\alpha x + \alpha y = cT(x) + T(y)$$

where the third equality is given by the fact that $c, \alpha \in K$ so $\alpha c = c\alpha$.

□

(b) Prove that K is isomorphic to a subfield of the ring $M_n(F)$ of $n \times n$ matrices over F. (For a review of the relationship between matrix rings and rings of linear transformations of a vector space, see §11.2.) Thus $M_n(F)$ contains a copy of every extension of F with degree $\leq n$.

Proof. Define $\varphi : K \to M_n(F)$ by $\alpha \mapsto \mathrm{Mat}(T_\alpha)$, where $T_\alpha(x) = \alpha x$ and Mat denotes the matrix representation of a linear map $K \to K$ with respect to some basis for K over F. Since T_α is an F-linear transformation of K, the Mat function is well-defined.

We will show that φ is a ring homomorphism, thus a field homomorphism: for any $\alpha, \beta, x \in K$,

$$\begin{aligned} \varphi(\alpha + \beta)(x) &= \mathrm{Mat}(T_{\alpha+\beta})(x) = (\alpha + \beta)(x) = \alpha x + \beta x \\ &= \mathrm{Mat}(T_\alpha)(x) + \mathrm{Mat}(T_\beta)(x) = (\varphi(\alpha) + \varphi(\beta))(x) \end{aligned}$$

and

$$\begin{aligned} \varphi(\alpha\beta)(x) &= \mathrm{Mat}(T_{\alpha\beta})(x) = \alpha\beta x \\ &= \mathrm{Mat}(T_\alpha)\,\mathrm{Mat}(T_\beta)(x) = (\varphi(\alpha) \circ \varphi(\beta))(x). \end{aligned}$$

Clearly, $\varphi \neq 0$, since $\varphi(1) = T_1$ is the identity map, which is nonzero. The image of a nonzero field homomorphism is a field, thus φ is an isomorphism onto a subfield of $M_n(F)$.

□

4. (Exercise 4 in DF §14.1.) Prove that $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{3})$ are not isomorphic.

Proof. Suppose that $\varphi : \mathbf{Q}(\sqrt{2}) \to \mathbf{Q}(\sqrt{3})$ is an isomorhpism. Then there is some unique $\alpha \in \mathbf{Q}(\sqrt{2})$ whose image is $\sqrt{3}$, so

$$\varphi(\alpha^2) = \varphi(\alpha)^2 = (\sqrt{3})^2 = 3.$$

However, we also have

$$\varphi(3) = \varphi(1 + 1 + 1) = 3\varphi(1) = 3.$$

Since φ is a bijection, this means that $\alpha^2 = 3$. We know $\alpha = a + b\sqrt{2}$ for some $a, b \in \mathbf{Q}$, so $(a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2} = 3$. Since the set $\{1, \sqrt{2}\}$ is linearly independent over $\mathbf{Q}$, this gives the system

$$\begin{cases} a^2 + 2b^2 = 3 \\ 2ab\sqrt{2} = 0 \end{cases}.$$

From the second equation, we know either $a = 0$ or $b = 0$. If $a = 0$, then the first equation gives $b^2 = \frac{3}{2}$, which has no rational solution for b. If $b = 0$, we obtain $a^2 = 3$, which also has no rational solutions for a. Therefore $\alpha \notin \mathbf{Q}(\sqrt{2})$, a contradiction.

□

5. (Exercise 7 in DF §14.1.) This exercise determines $\mathrm{Aut}(\mathbf{R}/\mathbf{Q})$.

(a) Prove that any $\sigma \in \mathrm{Aut}(\mathbf{R}/\mathbf{Q})$ takes squares to squares and takes positive reals to positive reals. Conclude that $a < b$ implies $\sigma(a) < \sigma(b)$ for every $a, b \in \mathbf{R}$.

Proof. For any $\alpha \in \mathbf{R}$, $\sigma(\alpha^2) = \sigma(\alpha)^2$ is a square. Thus σ takes squares to squares.

In $\mathbf{R}$, any positive real number x is the square of $\sqrt{x}$, which is also a real number. So $\sigma(x)$ is a square as well. Therefore, $\sigma(x)$ is nonnegative, since $\mathbf{R}$ contains no negative perfect squares. Since σ is bijective, the only element that maps to 0 is 0, thus $\sigma(x) \neq 0$ since x is strictly positive. So $\sigma(x)$ is positive, thus σ takes positive reals to positive reals.

□

(b) Prove that $-\frac{1}{m} < a - b < \frac{1}{m}$ implies $-\frac{1}{m} < \sigma(a) - \sigma(b) < \frac{1}{m}$ for every positive integer m. Conclude that σ is a continuous map on $\mathbf{R}$. (Recall that a map $f : \mathbf{R} \to \mathbf{R}$ is *continuous* if for every $a \in \mathbf{R}$ and every $\epsilon > 0$ there exists some $\delta > 0$ such that $|f(b) - f(a)| < \epsilon$ whenever $|b - a| < \delta$.)

Proof. Suppose $-\frac{1}{m} < a - b < \frac{1}{m}$. Then $a - b + \frac{1}{m} > 0$ and $\frac{1}{m} + b - a > 0$. By part (a), this means that $\sigma(a) - \sigma(b) + \sigma(\frac{1}{m}) > 0$ and $\sigma(\frac{1}{m}) + \sigma(b) - \sigma(a) > 0$. Since $\frac{1}{m}$ is rational and σ fixes rationals, $\sigma(\frac{1}{m}) = \frac{1}{m}$. So rearranging the inequalities gives $-\frac{1}{m} < \sigma(a) - \sigma(b) < \frac{1}{m}$.

Now, let $\epsilon > 0$. By the Archimedean Principle, there exists some positive integer m such that $\frac{1}{m} < \epsilon$. Let $\delta = \frac{1}{m}$. Whenever $|a - b| < \delta$, it follows that $|\sigma(a) - \sigma(b)| < \frac{1}{m} < \epsilon$ by the above paragraph. Therefore, σ is continuous.

□

(c) Prove that any continuous map $\mathbf{R} \to \mathbf{R}$ which is the identity on $\mathbf{Q}$ is the identity map; hence $\mathrm{Aut}(\mathbf{R}/\mathbf{Q}) = \{1\}$. (You may use without proof the fact that $\mathbf{Q}$ is dense in $\mathbf{R}$; that is, for every $a \in \mathbf{R}$ and every $\epsilon > 0$ there exists some $q \in \mathbf{Q}$ such that $|a - q| < \epsilon$.)

Proof. Let $x \in \mathbf{R}$. By definition, x is the limit of some Cauchy sequence $\{q_n\}$ in $\mathbf{Q}$. Suppose $f : \mathbf{R} \to \mathbf{R}$ is a continuous function that fixes $\mathbf{Q}$. Since f is continuous and q_n is convergent, $f(\lim q_n) = \lim f(q_n)$. Since f fixes $\mathbf{Q}$, we know $f(q_n) = q_n$. So

$$f(x) = f(\lim q_n) = \lim f(q_n) = \lim q_n = x$$

therefore f fixes $\mathbf{R}$ as well, since x was arbitrary. So f must be the identity.

We have shown that if $\sigma \in \mathrm{Aut}(\mathbf{R}/\mathbf{Q})$ is a continuous map that fixes $\mathbf{Q}$, then σ is the identity. So $\mathrm{Aut}(\mathbf{R}/\mathbf{Q}) = \{1\}$.

□

6. (Exercise 9 in DF §14.1.) Let k be a field, and let $k(t)$ denote the field of rational functions in t with coefficients in k. (In other words, $k(t)$ is the field of fractions of the polynomial ring $k[t]$. It is an extension of k of infinite degree.) Observe (but you need not prove) that the map $\phi : k(t) \to k(t)$ given by $\phi(r(t)) = r(t + 1)$ is an automorphism of $k(t)$. Determine (with proof) the fixed field of ϕ.

The fixed field of ϕ is the field of all $r \in k(t)$ that are periodic with a period of 1.

Proof. If r is periodic with a period of 1, then $\phi(r)(t) = r(t + 1) = r(t)$ for all t, thus $\phi(r) = r$.

Conversely, if r is not periodic with a period of 1, then for some t, $r(t) \neq r(t+1) = \phi(r)(t)$, thus $\phi(r) \neq r$.

□