MATH 7752 Homework 8

James Harbour

April 1, 2022

Problem 1

Note: Let K/F be a field extension. Consider the set $\mathrm{Aut}_F(K)$ consisting of all F-isomorphisms $\sigma : K \to K$. Such isomorphisms are called F-*automorphisms* of K. Note that $\mathrm{Aut}_F(K)$ forms a group under composition.

(a): Let F be a field and let $\overline{F}$ be an algebraic closure of F. Let $\sigma : \overline{F} \to \overline{F}$ be an F-embedding. Prove that $\sigma(\overline{F}) = \overline{F}$, and thus σ is an automorphism of $\overline{F}$.

Proof. Take $\alpha \in \overline{F}$. Then there exists a monic $f \in \overline{F}[x]$ such that $f(\alpha) = 0$. Since $\overline{F}$ is algebraically closed, there exist $\alpha_1 \cdots, \alpha_n \in \overline{F}$ (WLOG $\alpha_1 = \alpha$) such that

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

But then

$$(x - \sigma(\alpha_1)) \cdots (x - \sigma(\alpha_n)) = \widetilde{\sigma}(f) = f = (x - \alpha_1) \cdots (x - \alpha_n)$$

whence there exists some $i \in \{1, \dots, n\}$ such that $\sigma(\alpha_i) = \alpha$. □

(b): Prove that for any field F any two algebraic closures of F are F-isomorphic. **Hint:** Use the Main Extension Lemma.

Proof. Let K_1/F, K_2/F be two algebraic closures of F. By the main extension lemma, there exist F-embeddings $\sigma : K_1 \hookrightarrow K_2$ and $\sigma' : K_2 \hookrightarrow K_1$. Then $\sigma' \circ \sigma : K_1 \hookrightarrow K_1$ and $\sigma \circ \sigma' : K_2 \hookrightarrow K_2$ are both F-embeddings, whence by part (a) they are F-automorphisms. Thus σ and σ' are bijective, so K_1 and K_2 are F-isomorphic. □

Problem 2

For each of the following polynomials $f(x) \in \mathbb{Q}[x]$ let $K \subset \mathbb{C}$ be the splitting field of f over $\mathbb{Q}$.

(i) $f(x) = x^n - 1$, $n \geq 2$.

(ii) $f(x) = x^4 + 3x^3 + 4x^2 + 3x + 3$.

(iii) $f(x) = x^4 - 2$.

Find the degree $[K : \mathbb{Q}]$ and express K in the form $\mathbb{Q}(\alpha)$, or $\mathbb{Q}(\alpha, \beta)$. **Hint:** For (i) you can take a look at [DF. Section 13.6].

Solution.
(i): Let ζ_n be a primitive n^{th} root of unity (e.g. $\zeta_n = e^{\frac{2\pi i}{n}}$). We claim that $[K : \mathbb{Q}] = \varphi(n)$ and $K = \mathbb{Q}(\zeta_n)$ where φ is Euler's totient function.

As ζ_n is primitive, the set $\langle \zeta_n \rangle = \{\zeta_n^k : 0 \leq k < n\} \subseteq \mathbb{Q}(\zeta_n)$ has cardinality n and are all roots of f, so $K \subseteq \mathbb{Q}(\zeta_n)$. On the other hand, ζ_n is a root of f, so $\mathbb{Q}(\zeta_n) \subseteq K$. Thus $K = \mathbb{Q}(\zeta_n)$. Defining the n^{th} cyclotomic polynomial $\Phi_n(x)$ to be the product over all $(x - \varepsilon)$ where $\varepsilon \in \mathbb{C}$ is a primitive n^{th} root of unity, it follows that $\deg(\Phi_n) = \varphi(n)$. A result of Gauss (in DF Section 13.6) gives that Φ_n is in $\mathbb{Z}[x]$ and in fact irreducible, so $\mu_{\zeta_n,\mathbb{Q}} = \Phi_n$ whence $[K : \mathbb{Q}] = \deg(\mu_{\zeta_n,\mathbb{Q}}) = \deg(\Phi_n) = \varphi(n)$.

(ii): We claim that $K = \mathbb{Q}(i, \sqrt{3})$ and $[K : F] = 4$. Upon factoring $f(x) = (x^2 + 1)(x^2 + 3x + 3)$, we note that *a priori* $K = \mathbb{Q}(i, -i, -\frac{3}{2} + i\frac{\sqrt{3}}{2}, -\frac{3}{2} - i\frac{\sqrt{3}}{2})$. Let $\alpha_\pm = \pm i$ and $\beta_\pm = -\frac{3}{2} \pm i\frac{\sqrt{3}}{2}$. On one hand, it is clear that $K \subseteq \mathbb{Q}(i, \sqrt{3})$ as $\alpha_\pm, \beta_\pm \in \mathbb{Q}(i, \sqrt{3})$. On the other hand, we have that $i \in K$ so it suffices to show that $\sqrt{3} \in K$. Observe that

$$\alpha_+(2\beta_- + 3) = i\left(2\left(-\frac{3}{2} - i\frac{\sqrt{3}}{2}\right) + 3\right) = \sqrt{3}$$

so $K = \mathbb{Q}(i, \sqrt{3})$. Clearly $\mu_{\sqrt{3},\mathbb{Q}(i)} = \mu_{\sqrt{3},\mathbb{Q}} = x^2 - 3$, so $[K : \mathbb{Q}] = 4$.

(iii): We claim that $K = \mathbb{Q}(i, \sqrt[4]{2})$ and $[K : F] = 8$. Note that $x^4 - 2 = (x - \sqrt[4]{2})(x - i\sqrt[4]{2})(x + \sqrt[4]{2})(x + i\sqrt[4]{2})$, so *a priori* $K = \mathbb{Q}(\pm\sqrt[4]{2}, \pm i\sqrt[4]{2})$. On one hand, it is clear that $K \subseteq \mathbb{Q}(i, \sqrt[4]{2})$. On the other hand, $\sqrt[4]{2} \in K$ and $i = \frac{i\sqrt[4]{2}}{\sqrt[4]{2}} \in K$, so $\mathbb{Q}(i, \sqrt[4]{2}) \subseteq K$, whence $K = \mathbb{Q}(i, \sqrt[4]{2})$. Clearly $\mu_{\sqrt[4]{2},\mathbb{Q}(i)} = \mu_{\sqrt[4]{2},\mathbb{Q}} = x^4 - 2$, so $[K : \mathbb{Q}] = 8$.
$\square$

Problem 3

(a): Let F be a field. Prove that if $\mathrm{char}(F) = 0$, then there is an embedding $\mathbb{Q} \hookrightarrow F$, while if $\mathrm{char}(F) = p$, then there exists an embedding $\mathbb{F}_p \hookrightarrow F$.
Conclusion: The fields $\mathbb{Q}, \mathbb{F}_p$ are the smallest in each characteristic and we call them *prime fields*.

Proof. Let 1_F denote the multiplicative identity of F.

Case 1: $\mathrm{char}(F) = 0$. Let $\psi : \mathbb{Z} \to F$ be the ring homomorphism given by $\psi(n) = n \cdot 1_F$. As $\psi(\mathbb{Z} \setminus \{0\}) \in F^\times$, by the universal property of localization there exists a unique ring homomorphism $\sigma : \mathbb{Q} \to F$ such that $\sigma(\frac{n}{1}) = \psi(n) = n \cdot 1_F$ for all $n \in \mathbb{Z}$. As ψ is injective, it follows that σ is nonzero whence $\mathbb{Q}$ being a field implies that σ is an embedding.

Case 2: $\mathrm{char}(F) = p$. Define a map $\sigma : \mathbb{F}_p \to F$ by $\sigma(\overline{n}) = n \cdot 1_F$. To see that this map is well-defined, suppose that $\overline{n} = \overline{m}$, so $p|(n - m)$. Then $(n - m) \cdot 1_F = 0$, whence $n \cdot 1_F = m \cdot 1_F$. That this map is a ring homomorphism then follows from the fact that it is defined precisely by the $\mathbb{Z}$-module action on F. As $\sigma(\overline{1}) = 1_F \neq 0$, it follows that σ is injective so $\sigma : \mathbb{F}_p \to F$ is an embedding. $\square$

(b): Let F be a field. Prove that every automorphism $\sigma : F \to F$ of F is an F_0-automorphism, where F_0 is the prime subfield of F.

Proof. Let $K = \mathrm{Fix}(\sigma) = \{\alpha \in F : \sigma(\alpha) = \alpha\}$ be the fixed field of σ. As $K \neq 0$ and F_0 is the unique minimal subfield of F, it follows that $F_0 \subseteq K$, so σ is an F_0-automorphism of F. $\square$

Problem 4

The purpose of this problem is to prove that the group $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{R})$ is trivial by following the suggested steps. Let $\sigma : \mathbb{R} \to \mathbb{R}$ be an automorphism of $\mathbb{R}$.

1. Show that σ is strictly increasing.
2. Use the density of $\mathbb{Q}$ in $\mathbb{R}$ to show that σ is continuous at $x = 0$.
3. Deduce that σ is continuous on $\mathbb{R}$, and hence $\sigma(x) = x$.

Proof. (1): Suppose that $\alpha > 0$ and set $\beta = \sqrt{\alpha} > 0$. Then $\sigma(\beta) \neq 0$ so $\sigma(\alpha) = \sigma(\beta \cdot \beta) = \sigma(\beta)\sigma(\beta) = \sigma(\beta)^2 > 0$. Now, suppose that $x, y \in \mathbb{R}$ with $x < y$. Then $y - x > 0$, so

$$\sigma(y) = \sigma(y - x) + \sigma(x) > \sigma(x),$$

whence σ is strictly increasing.

(2): Let $(x_n)_{n=1}^{\infty}$ be a sequence in $\mathbb{R}$ such that $x_n \to 0$. By density of $\mathbb{Q}$ in $\mathbb{R}$, we may choose sequences $(a_n)_{n=1}^{\infty}, (b_n)_{n=1}^{\infty}$ in $\mathbb{Q}$ such that $a_n < x_n < b_n$ for all $n \in \mathbb{N}$, $a_n \to 0^-$, and $b_n \to 0^+$. As σ is strictily increasing, it follows that

$$a_n = \sigma(a_n) < \sigma(x_n) < \sigma(b_n) = b_n$$

for all $n \in \mathbb{N}$, whence by squeeze theorem $\sigma(x_n) \to 0 = \sigma(0)$. Thus σ is continuous at $x = 0$.

(3): Suppose that $x \in \mathbb{R}$ and let $(x_n)_{n=1}^{\infty}$ be a sequence in $\mathbb{R}$ such that $x_n \to x$. Then $x_n - x \to 0$, whence $\sigma(x - n) - \sigma(x) = \sigma(x_n - x) \to 0$ so $\sigma(x_n) \to \sigma(x)$. It follows that σ is continuous. Thus, σ is a strictly increasing, countinuous bijection of $\mathbb{R}$, so σ must be the identity. $\square$

Problem 5

(a): Let K/F be an algebraic extension. Prove that K/F is normal if and only if for any algebraic extension L/K and any F-automorphism $\sigma \in \operatorname{Aut}_F(L)$ we have $\sigma(K) = K$.

Proof.
$\underline{\Longrightarrow}$: Suppose that K/F is normal. Let L/K be an algebraic extension and $\sigma \in \operatorname{Aut}_F(L)$. Take $\alpha \in K$ and set $f = \mu_{\alpha,F} \in F[x]$. By normality of K/F, f splits over K so we may write

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i)$$

where $\alpha_i \in K$ and without loss of generality we take $\alpha_1 = \alpha$. Note that, as $\sigma|_F = id_F$, we have that

$$0 = \sigma(f(\alpha)) = f(\sigma(\alpha)) = \prod_{i=1}^{n}(\sigma(\alpha) - \alpha_i),$$

so $\sigma(\alpha) = \alpha_i$ for some $i \in \{1, \ldots, n\}$. Thus $\sigma(K) = K$.

$\underline{\Longleftarrow}$: Suppose that, for any algebraic extension L/K and any F-automorphism $\sigma \in \operatorname{Aut}_F(L)$, we have $\sigma(K) = K$. Let $\beta \in K$ and let $f = \mu_{\beta,F} \in F[x]$. Fix an algebraic closure $\overline{F}$ such that $K \subseteq \overline{F}$. Then we may write

$$f(x) = \prod_{i=1}^{n}(x - \beta_i)$$

where $\beta_i \in \overline{F}$ and without loss of generality we take $\beta_1 = \beta \in K$. By the simple extension lemma, there exists for each i an F-isomorphism $\sigma_i : F(\beta) \to F(\beta_i)$ such that $\sigma(\beta) = \beta_i$. Extend this map to an embedding $K \hookrightarrow \overline{F}$, we note that by assumption the image of this embedding is in fact K, so $\beta_i \in K$ for all i, whence $\mu_{\beta,F}$ splits over K.

$\square$

(b): Let K/F be a field extension, and let K_1 and K_2 be subfields of K containing F such that the extensions K_1/F and K_2/F are normal. Prove that the extensions K_1K_2/F and $K_1 \cap K_2/F$ are also normal.

Proof. Let L/K_1K_2 be an algebraic extension and $\sigma \in \mathrm{Aut}_F(K_1K_2)$. Then by normality of $K_1/F, K_2/F$ and part (a), $\sigma(K_1K_2) = \sigma(K_1)\sigma(K_2) = K_1K_2$. Thus, part (a) implies that K_1K_2/F is normal.

In a similar vein, let $L/K_1 \cap K_2$ be an algebraic extension. Then by normality of $K_1/F, K_2/F$ and part (a), $\sigma(K_1 \cap K_2) = \sigma(K_1) \cap \sigma(K_2) = K_1 \cap K_2$. Thus, part (a) implies that $K_1 \cap K_2/F$ is normal.

$\square$