Algebra II: Homework 10

Due on April 14, 2021

Professor Walton

Gabriel Gress

Last edited April 14, 2021

Problem 1

Claim. Let τ be the map $\tau : \mathbb{C} \to \mathbb{C}$ defined by $\tau(a+bi) = a - bi$. Prove that τ is an automorphism of $\mathbb{C}$, and then use this to determine the fixed field of τ on $\mathbb{C}$.

Proof. Observe that

$$\tau((a+bi)+(c+di)) = (a+c)-(b+d)i = \tau(a+bi)+\tau(c+di)$$
$$\tau((a+bi)(c+di)) = \tau((ac-bd)+(ad+cd)i) = (ac-bd)-(ad+cd)i = (a-bi)(c-di) = \tau(a+bi)\tau(c+di)$$

and hence τ is an automorphism of $\mathbb{C}$. Now we will show that the fixed field of τ is $\mathbb{R}$. Observe that

$$\tau(a+bi) = a - bi = a + bi \iff b = 0$$

which is exactly the space of $\mathbb{R}$. □

Problem 2

Claim.

(a). Determine the automorphisms of the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ explicitly.

(b). Show that $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$ is not the trivial group.

Proof. (a). We are looking for the automorphisms of $\mathbb{Q}(\sqrt[4]{2}$ that fix $\mathbb{Q}(\sqrt{2})$. Observe that the minimal polynomial for $\mathbb{Q}(\sqrt[4]{2})$ is $x^4 - 2$, which has roots in $\mathbb{Q}(\sqrt[4]{2})$ given by $\left\{\sqrt[4]{2}, -\sqrt[4]{2}\right\}$. Because the other two roots are complex and hence not in the space, we only have the two automorphisms: the identity automorphism, and the automorphism given by $\begin{cases} \sqrt[4]{2} \mapsto -\sqrt[4]{2} \\ -\sqrt[4]{2} \mapsto \sqrt[4]{2} \end{cases}$. Explicitly:

$$\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})) = \left\{\mathrm{Id}_{\mathbb{Q}(\sqrt[4]{2})}; \sigma : \sqrt[4]{2} \mapsto -\sqrt[4]{2}\right\}$$

(b). Observe that $\sqrt{2}$ is not a root of our minimal polynomial as given above. As a result, the automorphisms of $\mathbb{Q}\sqrt[4]{2}/\mathbb{Q}(\sqrt{2})$ are exactly the same as the automorphisms of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. Hence we see that the automorphism group is the finite group of order two as given above (and hence not the trivial group).

□

Problem 3

Claim. Let ζ_n be a primitive nth root of unity in $\mathbb{C}$. Show that $\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is an abelian group.

Proof. By construction any automorphism on the space fixes $\mathbb{Q}$. As a result, for any automorphism defined on $\varphi(\zeta_n)$ must satisfy $\varphi(\zeta_n)^n = \varphi(\zeta_n^n) = \varphi(1) = 1$. In other words, we can see that the automorphisms must permute the roots of unity. In other words, we can represent automorphisms of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ by

$$\varphi_i(\zeta_n) = \zeta_n^i.$$

Problem 3 continued on next page. . .

Now we simply check that

$$\varphi_i \varphi_j(\zeta_n) = \varphi_i(\zeta_n^j) = \zeta_n^{ji} = \zeta_n^{ij} = \varphi_j(\zeta_n^i) = \varphi_j \varphi_i(\zeta_n)$$

And hence we have that they must commute for all automorphisms on $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. □

Problem 4

Claim.

(a). Show that if the field K is generated over F by the elements $\alpha_1, \ldots, \alpha_n$, then an automorphism σ of K fixing F is uniquely determined by $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$.

(b). Let $G \leq \mathrm{Gal}(K/F)$ be a subgroup of the Galois group of the extension K/F and suppose $\sigma_1, \ldots, \sigma_k$ are generators for G. Show that the subfield E/K is fixed by G if and only if it is fixed by the generators $\sigma_1, \ldots, \sigma_k$.

Proof. (a). Let K/F be a field extension generated by $\alpha_1, \ldots, \alpha_n$, let σ be an automorphism of K that fixes F, and let $x \in K/F$ be given by $x = \lambda_1 \alpha_1 + \ldots + \lambda_n \alpha_n$. Then

$$\sigma(x) = \sigma(\sum_{i=1}^n \lambda_i \alpha_i) = \sum_{i=1}^n \lambda_i \sigma(\alpha_i)$$

and hence if F is to be fixed, then $\{\lambda_i\}$ is uniquely determined for a given automorphism.

(b). Suppose E/F is fixed by $G \leq \mathrm{Gal}(K/F)$ generated by $\sigma_1, \ldots, \sigma_k$. It immediately follows that if it is fixed by G it must be fixed by the generators themselves. The reverse direction does not follow as directly: if E/F is fixed by $\sigma_1, \ldots, \sigma_k$ individually, then consider $\sigma \in G$. Observe that $\sigma \in \mathrm{Aut}(K/F)$, which implies that σ fixes K. Because $E/F \subset K/F$, it must hold that σ fixes E, and hence we are done.

□

Problem 5

Claim. Let $F \subset E \subset K$ be a composition of field extensions so that E is normal over F. Prove that if $\sigma \in \mathrm{Aut}(K/F)$, then $\sigma(E) = E$.

Proof. Let $\sigma \in \mathrm{Aut}(K/F)$ be given. K/F is hence Galois, and so by a proposition from class, we know that K is the splitting field of a separable polynoimal $p \in F[x]$. Let $\alpha_1, \ldots, \alpha_n$ be roots of p, all distinct. Because α_i generate K/F, there exists a subset of $\{\alpha_i\}$ that generates $E \subset F$ which we will denote by $\alpha_1', \ldots, \alpha_m'$ with $m \leq n$. Because E/F is normal we know that α_i' must be the roots of a separable polynomial $p' \in F[x]$ (as the α_i' are distinct). This gives us that E/F is Galois, and hence $\sigma(E) = E$ as desired. □

Problem 5 continued on next page...

Problem 6

Claim.

(a). Prove that any $\sigma \in \text{Aut}(\mathbb{R}/\mathbb{Q})$ takes squares to squares and positive reals to positive reals. Use this to conclude that $a < b$ implies $\sigma a < \sigma b$ for $a, b \in \mathbb{R}$.

(b). Prove that $-\frac{1}{m} < a - b < \frac{1}{m}$ implies $-\frac{1}{m} < \sigma a - \sigma b < \frac{1}{m}$ for every positivfe integer m. Conclude that σ is the continuous map on $\mathbb{R}$.

(c). Prove that any continous map on $\mathbb{R}$ which is the identity of $\mathbb{Q}$ is the identity map, and hence $\text{Aut}(\mathbb{R}/\mathbb{Q}) = 1$.

Proof. (a). Let $\sigma \in \text{Aut}(\mathbb{R}/\mathbb{Q})$ be given, and let $x \in \mathbb{R}$ be an element which can be expressed as $x = y^2$ for some $y \in \mathbb{R}$. Of course it then holds that $\sigma(x) = \sigma(y^2) = \sigma(y)^2$. Now let x be an arbitrary positive real number. By the property of $\mathbb{R}$, $\sqrt{x}$ is well defined and hence $x = \sqrt{x}^2$. Hence

$$\sigma(x) = \sigma(\sqrt{x})^2$$

which must be greater than zero, as $\sqrt{x} \neq 0$. Now let $a < b$ be given. Observe that $b - a$ is a positive real number, and hence

$$b - a > 0 \implies \sigma(b-a) > 0 \implies \sigma(b) - \sigma(a) > 0 \implies \sigma(a) < \sigma(b)$$

as desired.

(b). Now suppose that for some positive integer m we have

$$-\frac{1}{m} < a - b < \frac{1}{m}.$$

Then

$$-1 < m(a-b) < 1 \implies \sigma(-1) < \sigma(m(a-b)) < \sigma(1) \implies -1 < \sigma(m(a-b)) < 1$$
$$\implies -\frac{1}{m} < \sigma(a) - \sigma(b) < \frac{1}{m}.$$

Now we argue that this gives continuity. For every $\varepsilon > 0$ there exists a positive integer m such that $\frac{1}{m} < \varepsilon$ by the Archimedean property. Hence if $|a - b| < \frac{1}{m}$, then $|\sigma(a) - \sigma(b)| < \frac{1}{m} < \varepsilon$, and hence we can choose our delta to be $\frac{1}{m}$, giving us continuity as defined on $\mathbb{R}$.

(c). This directly follows from the fact that continuous functions that agree on dense sets of a space must agree on the whole space. As a result, if a continuous map is identity on $\mathbb{Q}$, it must be identity on $\mathbb{R}$, as $\mathbb{Q}$ is dense in $\mathbb{R}$.

$\square$