Homework 4

Kevin Guillen

MATH 202 — Algebra III — Spring 2022

Problem 14.1.5 Prove that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.

Proof. Let us assume that they are indeed isomorphic, that would then mean there exists an isomorphism between these two fields. Let us denote it by φ. Recall that isomorphisms are injective and surjective homomorphisms. Meaning we can consider we have,

$$\varphi(\sqrt{2}) = a + b\sqrt{3}$$

where $a, b \in \mathbb{Q}$. We know though that $b \neq 0$ since we have $\varphi(a)$ and φ is injective. Now we can consider,

$$\begin{aligned} 2 = \varphi(2) &= \varphi(\sqrt{2}^2) && \varphi \text{ is multiplicative} \\ &= \varphi(\sqrt{2})^2 \\ &= (a + b\sqrt{3})^2 \\ &= a^2 + 3b^2 + 2ab\sqrt{3} \end{aligned}$$

if $a \neq 0$ too, we have,

$$\begin{aligned} 2 &= a^2 + 3b^2 + 2ab\sqrt{3} \\ 2 - a^2 - ab^2 &= 2ab\sqrt{3} \\ \frac{2 - a^2 - ab^2}{2ab} &= \sqrt{3} \end{aligned}$$

meaning that $\sqrt{3} \in \mathbb{Q}$, since a and b are rationals and $\mathbb{Q}$ is a field, which is a contradiction. Therefore $a = 0$ and we have,

$$\begin{aligned} 2 &= 3b^2 \\ \frac{2}{3} &= b^2 \\ \frac{\sqrt{2}}{\sqrt{3}} &= b \end{aligned}$$

meaning that $\frac{\sqrt{2}}{\sqrt{3}} \in \mathbb{Q}$ which is also a contradiction. We already covered why b cant be 0, thus by contradiction there can be no isomorphism between $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$, meaning they are not isomorphic. $\square$

Problem 14.1.5 Determine the automorphisms of the extensions explicitly of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$.

Proof. We know the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}(\sqrt{2})$ is $x^2 - \sqrt{2}$. Where this equation has roots $\sqrt[4]{2}$ and $-\sqrt[4]{2}$ meaning we have the automorphisms 1 and σ where,

$$\begin{aligned} 1(a + b\sqrt[4]{2}) &= a + b\sqrt[4]{2} \\ \sigma(a + b\sqrt[4]{2}) &= a - b\sqrt[4]{2} \end{aligned}$$

Meaning then that $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})) \cong \mathbb{Z}/2\mathbb{Z}$ $\square$

Problem 14.1.7 This exercise determines $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$.

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

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

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

(a) *Proof.* Let σ be as defined in the problem statement. Now let $c \in \mathbb{R}_+$ we have then that $\sqrt{c} \in \mathbb{R}$, and we know $c = \sqrt{c}\sqrt{c}$. Now notice,

$$\begin{aligned} \sigma(c) &= \sigma(\sqrt{c}\sqrt{c}) \\ &= \sigma(\sqrt{c})\sigma(\sqrt{c}) \end{aligned}$$

which is a square and also a positive real number as desired.

If $a < b$ we have then by definition we have that $0 < b - a$ applying σ to both we have,

$$\begin{aligned} \sigma(0) &< \sigma(b - a) \\ 0 &< \sigma(b) - \sigma(a) \\ \sigma(a) &< \sigma(b). \end{aligned}$$

as desired. $\square$

(b) *Proof.* Due to the last part we know if $-\frac{1}{m} < a - b < \frac{1}{m}$ then we have,

$$\sigma(-1/m) < \sigma(a - b) < \sigma(1/m)$$

recall that σ fixes $\mathbb{Q}$ and $1/m$ is rational so,

$$-\frac{1}{m} < \sigma(a - b) < \frac{1}{m} \qquad \sigma \text{ is additive}$$

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

as desired.

For σ to be continuous we must have that for any $\varepsilon > 0$ there exists $\delta > 0$ such that,

$$|a - b| < \delta \implies |\sigma(a) - \sigma(b)| < \varepsilon.$$

We see though that we can let $\delta = \varepsilon$ and the implication we just proved proves the continuity of σ. ☐

(c) *Proof.* Now let σ be any continuous map on $\mathbb{R}$ that fixes $\mathbb{Q}$. We know then from real analysis that for any $x \in \mathbb{R}$ there exists a sequence (x_n) such that $\lim_{n\to\infty} x_n = x$ where $x_n \in \mathbb{Q}$. By definition of continuity we have then that,

$$\lim_{n\to\infty} \sigma(x_n) = \sigma(\lim_{n\to\infty} x_n)$$

we know though that σ fixes $\mathbb{Q}$ so $\sigma(x_n) = x_n$ for all x_n, so we have,

$$\begin{aligned} \lim_{n\to\infty} x_n &= \sigma(\lim_{n\to\infty} x_n) \\ x &= \sigma(x) \end{aligned}$$

therefore any continuous map on $\mathbb{R}$ that fixes $\mathbb{Q}$ is simply the identity map of $\mathbb{R}$. ☐

Problem 14.1.10 Let K be an extension of the field F. Let $\varphi : K \to K'$ be an isomorphism of K with a field K' which maps F to the subfield F' of K'. Prove that the map $\sigma \mapsto \varphi\sigma\varphi^{-1}$ defines a group isomorphism $\mathrm{Aut}(K/F) \xrightarrow{\sim} \mathrm{Aut}(K'/F')$

Proof. Let the map π be defined as,

$$\begin{aligned} \pi : \mathrm{Aut}(K/F) &\to \mathrm{Aut}(K'/F') \\ \sigma &\mapsto \varphi\sigma\varphi^{-1}. \end{aligned}$$

Let $\sigma_1, \sigma_2 \in \mathrm{Aut}(K/F)$ we see that,

$$\begin{aligned} \pi(\sigma_1\sigma_2) &= \varphi\sigma_1\sigma_2\varphi^{-1} \\ &= \varphi\sigma_1 1 \sigma_2\varphi^{-1} \\ &= \varphi\sigma_1\varphi^{-1}\varphi\sigma_2\varphi^{-1} \\ &= \pi(\sigma_1)\pi(\sigma_2) \end{aligned}$$

π is indeed a group homomorphism.

Let σ_1 and σ_2 be as before, note that

$$\pi(\sigma_1) = \pi(\sigma_2)$$

$$\begin{aligned}\varphi\sigma_1\varphi^{-1} &= \varphi\sigma_2\varphi^{-1}\\ \varphi\sigma_1 &= \varphi\sigma_2\\ \sigma_1 &= \sigma_2\end{aligned}$$

and therefore π is injective.

Let $\delta \in \mathrm{Aut}(K'/F')$ then let $\sigma = \varphi^{-1}\delta\varphi$ we see that,

$$\begin{aligned}\pi(\sigma) &= \varphi\varphi^{-1}\delta\varphi\varphi^{-1}\\ &= 1\delta 1\\ &= \delta\end{aligned}$$

we have then that π is also surjective.

All together that means the given map π is a group isomorphism. $\square$

Problem 14.2.4 Let p be a prime. Determine the elements of the Galois group of $x^p - 2$.

Proof. Let $\theta = \sqrt[p]{2}$ (the real value) and ζ_p be a principle p^{th} root of unity. Clearly $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ and by Eisenstein $x^p - 2$ is irreducible, so the splitting field will be of degree $\varphi(p)p = (p-1)p$.

An element of the Galois group is of course defined by where it maps these generators, meaning θ can be mapped to $\theta\zeta^n$ for $n = 1, 2, \dots, p$, and ζ_p can be mapped to $(\zeta_p)^n$ for $n = 1, 2, \dots, p-1$.

Because the order is $p(p-1)$ and we see the the number of possibilities is $p(p-1)$ we have that all the maps above are elements of the Galois group. $\square$

Problem 14.2.5 Prove that the Galois group of $x^p - 2$ for p a prime is isomorphic to the group of matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ where $a, b \in \mathbb{F}_p$, $a \neq 0$.

Proof. Let θ and ζ_p be as before. We know then the element of the group are $\sigma_{(m,n)}$ where,

$$\sigma_{(m,n)} = \begin{cases} \zeta_p \mapsto \zeta^m & m = 1, 2, \dots, p-1 \\ \theta \mapsto \zeta^n & n = 1, 2, 3 \dots, p-1 \end{cases}$$

Our claim now is that the correspondence between this group and the one defined in the problem statement are isomorphic through,

$$\pi : \sigma_{(m,n)} \mapsto \begin{pmatrix} m & n \\ 0 & 1 \end{pmatrix}$$

It is clear why these two are bijective all that needs to be shown is that it is a group homomorphism. Notice the following though,

$$\sigma_{(m,n)}\sigma_{(m',n')}(\zeta_p) = \zeta_p^{mm'}$$

and

$$\begin{aligned}\sigma_{(m,n)}\sigma_{(m',n')}(\theta) &= \sigma_{(m,n)}(\theta\zeta_p^{n'}) \\ &= \theta\zeta_p^n\zeta_p^{mn'} \\ &= \theta\zeta^{n+mn'}\end{aligned}$$

and

$$\begin{pmatrix} m & n \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} m' & n' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} mm' & n+mn' \\ 0 & 1 \end{pmatrix}$$

we we have then that π is indeed a homomorphism and therefore an isomorphism as desired. $\square$

Problem 14.2.6 Let $K = \mathbb{Q}(\sqrt[8]{2}, i)$ and let $F_1 = \mathbb{Q}(i)$, $F_2 = \mathbb{Q}(\sqrt{2})$, $F_3 = \mathbb{Q}(\sqrt{2})$. Prove that $Gal(K/F_1) \cong Z_8$, $Gal(K/F_2) \cong D_8$, $Gal(K/F_3) \cong Q_8$.

Proof. Let $zeta_8$ be the 8th primitive root of unity, similarly to a previous problem we have that,

$$Gal(\mathbb{Q}(\sqrt[8]{2}, i)/\mathbb{Q}) = \left\langle \sigma, \tau \mid \sigma^8 = \tau^2, \sigma\tau = \tau\sigma^3 \right\rangle$$

σ and τ defined as,

$$\tau : \begin{cases} \sqrt[8]{2} \mapsto \sqrt[8]{2} \\ i \mapsto -i \\ \zeta_8 \mapsto \zeta_8^7 \end{cases} \qquad \sigma : \begin{cases} \sqrt[8]{2} \mapsto \zeta_8\sqrt[8]{2} \\ i \mapsto i \\ \zeta_8 \mapsto \zeta_8^5 \end{cases}$$

We see that F_1 then is the fixed field of $H_1 = \langle\sigma\rangle$, F_2 the fixed field of $H_2 = \left\langle\sigma^2, \tau\right\rangle$, and F_3 the fixed field of $\left\langle\sigma^2, \tau\sigma^2\right\rangle$. We know from Dummit and Foote though (Corollary 11) that $Gal(K/F_n) = H_n$ for $n = 1, 2, 3$.

H_1 is of order 8 containing an element of order 8 because recall that $\sigma^8 = 1$, giving us that H_1 is isomorphic to Z_8 as desired.

Note that $\sigma^2\tau = \sigma\sigma\tau = \sigma\tau\sigma^3 = \sigma\tau^{-1}$ meaning that

$$H_2 = \left\langle \sigma^2, \tau \mid (\sigma^2)^4 = \tau^2 = 1,\ \sigma\tau = \tau\sigma^{-1} \right\rangle$$

but these generators and their relations are what define the dihedral group of order 8, thus $H_2 \cong D_8$.

Finally we have that $(\sigma^2)^4 = 1, (\tau\sigma^3)^4 = 1$, $\sigma^2(\tau\sigma^3) = (\tau\sigma^3)^{-1}\sigma^2$ and $(\sigma^2)^2 = \sigma^4(\tau\sigma^3)^2$ giving us that,

$$H_3 = \left\langle \sigma^2, \tau\sigma^3 \mid (\sigma^2)^4 = (\tau\sigma^3)^4, \sigma^2(\tau\sigma^3) = (\tau\sigma^3)^{-1}\sigma^2, (\sigma^2)^2 = (\tau\sigma^3)^2 \right\rangle$$

showing us that $H_3 \cong Q_8$ as desired. $\square$

Problem 14.2.10 Determine the Galois group of the splitting field over $\mathbb{Q}$ of $x^8 - 3$.

Proof. Let ζ_8 be as usual, we have the 8 roots of the given polynomial to be $\zeta_8^n \sqrt[8]{3}$ where $n = 0, 1, \ldots, 7$. Therefore we have that the splitting field is $\mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i)$. We note that $x^8 - 3$ is Eisenstein so it is irreducible. Meaning the first extension will be of degree 8.

Now assuming that $x^2 - 2$ is reducible over $\mathbb{Q}(\sqrt[8]{3})$ gives us that,

$$(a_7 \sqrt[8]{3}^7 + \cdots + a_1 \sqrt[8]{3} + a_0)^2 = 2$$

now we see the coefficient of the basis element 1 to be,

$$3a_4^2 + 6a_3a_5 + 6a_2a_6 + 6a_1a_7 + a_0^2 = 2.$$

The integral domain of the element of the form $b_7 \sqrt[8]{3}^7 + \cdots + b_1 \sqrt[8]{3} + b_0$ for $b_i \in \mathbb{Z}$ has field of fractions $\mathbb{Q}(\sqrt[8]{3})$, and that they contain each other. So we can assume then that $a_i \in \mathbb{Z}$ and if we mod 3 the equality becomes impossible. Giving us that $\mathbb{Q}(\sqrt[8]{3}, \sqrt{2})$ is of degree 16 and because it is a field it is contained in $\mathbb{R}$. Giving us then that $K = \mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i)$ is of degree 32 over $\mathbb{Q}$.

We have $32 = 2 \cdot 2 \cdot 8$ permutations of the roots and all are automorphisms so $\pi : \sqrt[8]{3} \mapsto \zeta_8 \sqrt[8]{3}$, $\tau : \sqrt{2} \mapsto -\sqrt{2}$, and $\sigma : i \mapsto -i$ generate $\mathrm{Gal}(K/\mathbb{Q})$.

We also note that

$$\begin{aligned} \pi^8 &= \tau^2 = \sigma^2 \\ \tau\sigma &= \sigma\tau \\ \tau\pi &= \pi^5\tau \\ \sigma\pi &= \pi^3\sigma \end{aligned}$$

these relations on a free group of three generators is suffice to write any element in the form $\pi^x \tau^y \sigma^z$ which yield 32 combinations, which is,

$$\mathrm{Gal}(K/\mathbb{Q}) = \langle \pi, \tau, \sigma \mid \pi^8 = \tau^2 = \sigma^2 = 1, \tau\sigma = \sigma\tau, \tau\pi = \pi^5\tau, \sigma\pi = \pi^3\sigma \rangle$$

Finally, notice that $7^2 \equiv 5^2 \equiv 3^2 \equiv 1 \bmod 8$ so $\mathrm{Aut}(Z_8) = Z_2^2$, letting f be the isomorphism between the two groups and letting x generate Z_8 and $y, z \in Z_2^2$ such that $f(y)(x) = x^5$ and $f(z)(x) = x^3$ we see these elements have the same relations that $Z_2^2 \rtimes_f Z_8$ is of order 32.

Therefore $\mathrm{Gal}(K/\mathbb{Q}) = Z_2^2 \rtimes_f Z_8$ $\square$

Problem 14.2.14 Show that $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$ is a cyclic quartic field, i.e., is a Galois extension of degree 4 with cyclic Galois group.

Proof. Let $K = \mathbb{Q}(\sqrt{2 + \sqrt{2}})$ which is a field. For it to be Galois it must contain all the conjugates of the generator. The generator satisfies,

$$\begin{aligned} x &= \sqrt{2 + \sqrt{2}} \\ x^2 - 2 &= \sqrt{2} \end{aligned}$$

$$(x^2-2)^2-2=0$$

we see that x^4-4x^2+2 is Eisenstein and therefore irreducible, so it must be the minimal polynomial of the generator. We then see all the conjugates are $\pm\sqrt{2\pm\sqrt{2}}$. Now we want to show that K contains all of them. We have that,

$$\sqrt{2-\sqrt{2}} = \frac{\sqrt{4-2}}{\sqrt{2+\sqrt{2}}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}$$

Note though that $\sqrt{2}\in K$ thereby showing that $\sqrt{2-\sqrt{2}}\in K$. Because K is a field we have the others through additive inverses, meaning then that K is Galois over $\mathbb{Q}$. From what we have already shown it is clear $[K:\mathbb{Q}]=4$. Meaning the Galois group is also of size 4, now consider the automorphism

$$\sigma(\sqrt{2+\sqrt{2}}) = \sqrt{2-\sqrt{2}}$$

if we apply this twice we see that,

$$\begin{aligned}
\sigma^2(\sqrt{2+\sqrt{2}}) &= \sigma(\sqrt{2-\sqrt{2}}) \\
&= \sigma\left(\frac{\sqrt{2+\sqrt{2}}^2-2}{\sqrt{2+\sqrt{2}}}\right) \\
&= \frac{\sigma(\sqrt{2+\sqrt{2}})^2-2}{\sigma(\sqrt{2+\sqrt{2}})} \\
&= \frac{\sqrt{2-\sqrt{2}}^2-2}{\sqrt{2-\sqrt{2}}} \\
&= \frac{-\sqrt{2}}{\sqrt{2-\sqrt{2}}}
\end{aligned}$$

which is not equal to $\sqrt{2+\sqrt{2}}$. This means then that σ is an automorphism of order 4. Therefore the Galois group is actually a cyclic group of order 4. $\square$