Graded

1. (14.2.13) Prove that if the Galois group of the splitting field of a cubic over $\mathbb{Q}$ is the cyclic group of order 3 then all the roots of the cubic are real.

   Proof. We prove the contrapositive. Suppose $f(x) \in \mathbb{Q}[x]$ has one real root and two complex roots $z, \overline{z}$ (where $\overline{z}$ is the complex conjugate of z), and let K be the splitting field of $f(x)$. We show that $\mathrm{Gal}(K/\mathbb{Q})$ has an order 2 element: let $\tau\colon K \to K$ be defined so that it is the identity on $\mathbb{Q}$ and r, but sends z to $\overline{z}$ (and sending $\overline{z}$ to z since complex conjugation is an involution). Observe that τ is its own left and right inverse so τ is a bijection; it is known that complex conjugation respects sums, differences, products, and quotients. Hence τ is an automorphism of K fixing $\mathbb{Q}$, and since it is its own inverse it has order 2. It follows that $\mathrm{Gal}(K/\mathbb{Q})$ could not be the cyclic group of order 3 (2 does not divide 3). □

2. (14.2.16)

   (a) Prove that $x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$.

   Proof. The polynomial $x^4 - 2x^2 - 2$ is Eisenstein at $p = 2$. □

   (b) Show the roots of this quartic are

   $$\alpha_1 = \sqrt{1+\sqrt{3}} \quad \alpha_2 = \sqrt{1-\sqrt{3}} \quad \alpha_3 = -\sqrt{1+\sqrt{3}} \quad \alpha_4 = -\sqrt{1-\sqrt{3}}.$$

   Proof. Multiply: $(x-\alpha_1)(x-\alpha_3)(x-\alpha_2)(x-\alpha_4) = [x^2-(1+\sqrt{3})][x^2-(1-\sqrt{3})] = x^4 - 2x^2 - 2$. □

   (c) Let $K_1 = \mathbb{Q}(\alpha_1)$ and $K_2 = \mathbb{Q}(\alpha_2)$. Show that $K_1 \neq K_2$, and $K_1 \cap K_2 = \mathbb{Q}(\sqrt{3}) = F$.

   Proof. Observe $\alpha_1 \in \mathbb{R}$ but $\alpha_2 \notin \mathbb{R}$ since $\sqrt{3} > 1$. It follows that $K_1 \neq K_2$. Observe that $\alpha_1^2 - 1 = 1 - \alpha_2^2 = \sqrt{3} \in K_1 \cap K_2$ so that $\mathbb{Q}(\sqrt{3}) \subseteq K_1 \cap K_2$ (a basis for $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$ is $\{1, \sqrt{3}\}$). But $x^4 - 2x^2 - 2$ is monic and irreducible with α_1 as a root so it is its minimal polynomial. It follows that K_1 is a degree 4 extension of $\mathbb{Q}$ containing $K_1 \cap K_2$. Since $K_1 \neq K_2$ and $\mathbb{Q}(\sqrt{3})$ is a degree 2 extension of $\mathbb{Q}$, it follows that $2 \leq [K_1 \cap K_2\colon \mathbb{Q}] < 4$. It follows that $2 = [K_1 \cap K_2\colon \mathbb{Q}] = [K_1 \cap K_2\colon \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3})\colon \mathbb{Q}]$, so $[K_1 \cap K_2\colon \mathbb{Q}(\sqrt{3})] = 1$ and so $K_1 \cap K_2 = \mathbb{Q}(\sqrt{3})$ as desired. □

   (d) Prove that K_1, K_2 and K_1K_2 are Galois over F with $\mathrm{Gal}(K_1K_2/F)$ the Klein 4-group. Write out the elements of $\mathrm{Gal}(K_1K_2/F)$ explicitly. Determine all subgroups of the Galois group and give their corresponding fixed subfields of K_1K_2 containing F.

   Proof. Observe that K_1 is the splitting field of $x^2-(1+\sqrt{3})$ and K_2 is the splitting field of $x^2-(1-\sqrt{3})$. Further see that $K_1K_2 = \mathbb{Q}(\alpha_1, \alpha_2)$ is the splitting field for $[x^2-(1+\sqrt{3})][x^2-(1-\sqrt{3})] = x^4-2x^2-2$; the aforementioned polynomials are separable so K_1, K_2 and K_1K_2 are Galois over F.

We write down generators for $\mathrm{Gal}(K_1K_2/F)$:

$$\sigma\colon \begin{cases} \alpha_1 \mapsto \alpha_1 \\ \alpha_2 \mapsto \alpha_4 = -\alpha_2 \end{cases} \qquad \tau\colon \begin{cases} \alpha_1 \mapsto \alpha_3 = -\alpha_1 \\ \alpha_2 \mapsto \alpha_2 \end{cases} \qquad \text{see also} \quad \sigma\tau\colon \begin{cases} \alpha_1 \mapsto \alpha_3 = -\alpha_1 \\ \alpha_2 \mapsto \alpha_4 = -\alpha_2 \end{cases}$$

(.) Observe that σ, τ, and $\sigma\tau$ have order 2 so that $\mathrm{Gal}(K_1K_2/F) = \langle \sigma, \tau \mid \sigma^2 = \tau^2 = (\sigma\tau)^2 = \mathrm{id}_{K_1K_2} \rangle$ which is a presentation for the Klein 4-group. The subgroups of the Galois group are copies of Z_2, given by $\langle\sigma\rangle, \langle\tau\rangle$, and $\langle\sigma\tau\rangle$. As σ fixes α_1 it follows that $(K_1K_2)^{\langle\sigma\rangle} = K_1$ and similarly τ fixes α_2 so that $(K_1K_2)^{\langle\tau\rangle} = K_2$. Observe that $\sigma\tau$ fixes $\alpha_1\alpha_2$ so that $(K_1K_2)^{\langle\sigma\tau\rangle} = F(\alpha_1\alpha_2)$. The trivial subgroup of course fixes K_1K_2 and the whole group fixes F (recall $\alpha_1^2 - 1 = 1 - \alpha_2^2 = \sqrt{3}$). □

(e) Prove that the splitting field of $x^4 - 2x^2 - 2$ over $\mathbb{Q}$ is of degree 8 with dihedral Galois group.

Proof. With $x^4 - 2x^2 - 2$ separable and K_1K_2 its splitting field we show that $\mathrm{Gal}(K_1K_2/\mathbb{Q})$ is the dihedral group of order 8. First see that there are exactly 8 automorphisms: F is a degree 2 extension of $\mathbb{Q}$, and K_1 is a degree 2 extension of F ($x^2 - (1+\sqrt{3})$ is irreducible over F). Then K_1K_2 is a degree 2 extension of K_1 ($x^2 - (1-\sqrt{3})$ is irreducible over K_1 since it has two complex roots), so $[K_1K_2\colon \mathbb{Q}] = 8$. Subgroups of Abelian groups are normal, so the Galois group $\mathrm{Gal}(K_1K_2/\mathbb{Q})$ could not be Abelian since we have a non-Galois extension K_1 over $\mathbb{Q}$ (intermediate Galois extensions correspond to normal subgroups, and $x^4 - 2x^2 - 2$ has complex roots which are not in K_1). But the only non-Abelian groups of order 8 are Q_8 and D_8. But Q_8 does not have the Klein 4-group as a subgroup so the Galois group must be D_8. □

Additional Problems

1. (14.2.6) Let $K = \mathbb{Q}(\sqrt[8]{2}, i)$ and let $F_1 = \mathbb{Q}(i)$, $F_2 = \mathbb{Q}(\sqrt{2})$, $F_3 = \mathbb{Q}(i\sqrt{2})$. Prove that $\mathrm{Gal}(K/F_1) \cong Z_8$, $\mathrm{Gal}(K/F_2) \cong D_8$, $\mathrm{Gal}(K/F_3) \cong Q_8$.

   Proof. From the section of the example on page 578 which enumerates all the automorphisms of $\mathbb{Q}(\sqrt[8]{2}, i)$, we pick out exactly the ones which fix the generators of the fields above. Observe for F_1, the automorphisms fixing it are exactly the powers of σ, which form a group isomorphic to Z_8. The automorphisms fixing $\sqrt{2} = \theta^4$ are any which sends θ to $\zeta^a\theta$ with 8 dividing $4a$. The group of these automorphisms is generated by τ and σ^2; the relation we obtain is that $\tau^2 = (\sigma^2)^4 = \mathrm{id}_K$ so that the group is the dihedral group of order 8. Lastly, elements fixing $i\sqrt{2}$ are even powers of σ and $\tau\sigma^a$ for odd a. There is an isomorphism which I write using ordered lists: $\{1, -1, i, -i, j, -j, ij, -ij\} \leftrightarrow \{\sigma^8, \sigma^4, \sigma^2, \sigma^6, \tau\sigma, \tau\sigma^5, \tau\sigma^7, \tau\sigma^3\}$. Checking with the established relations in the parent group, we obtain Q_8. □

2. (14.2.7) Determine all the subfields of the splitting field of $x^8 - 2$ which are Galois over $\mathbb{Q}$.

Proof. We only need to identify the normal subgroups of the quasidihedral group of order 16. These are (one may obtain these by brute force and by using other useful theorems from group theory): $\langle\sigma^4\rangle, \langle\sigma^2\rangle, \langle\sigma\rangle, \langle\sigma^4, \tau\rangle, \langle\sigma^2, \tau\rangle$, and 1. These correspond to the subfields $\mathbb{Q}(i, \sqrt[4]{2}), \mathbb{Q}(i, \sqrt{2}), \mathbb{Q}(i), \mathbb{Q}(\sqrt[4]{2}), \mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(i, \sqrt[8]{2})$. □

3. (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. Observe that for α_i Galois conjugates of $\sqrt{s+\sqrt{2}}$, the product $\prod_{i=1}^{4}(x-\alpha_i) = x^4 - 4x^2 + 2$, which is separable and Eisenstein at $p = 2$ and hence irreducible. It is monic so it is the minimal polynomial of $\sqrt{2+\sqrt{2}}$.

We show that $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ is the splitting field for this polynomial by obtaining the other conjugates, namely $\sqrt{2-\sqrt{2}}$: Observe that for $\alpha_1 = \sqrt{2+\sqrt{2}}$, we have $\sqrt{2} = \alpha_1^2 - 2 \in K$ so that the quotient $\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} = \sqrt{2-\sqrt{2}} \in K$ as desired. Hence K is a degree 4 Galois extension of $\mathbb{Q}$.

Now we show that there is an automorphism of order 4 so that $\mathrm{Gal}(K/\mathbb{Q})$ is not the Klein 4-group: Take the map f sending $\sqrt{2+\sqrt{2}}$ to $\sqrt{2-\sqrt{2}}$; it follows that f sends $\sqrt{2}$ to $-\sqrt{2}$. Furthermore, f sends $\sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}$ to $\frac{-\sqrt{2}}{\sqrt{2-\sqrt{2}}} = -\sqrt{2+\sqrt{2}}$, which is sent to $-\sqrt{2-\sqrt{2}}$, sent back to $\sqrt{2+\sqrt{2}}$. Thus f has order 4. It follows that $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic of order 4. □

4. (Hilbert's Theorem 90 and Pythagorean Triples) Let K/F be Galois. For $\alpha \in K$, we define the norm of α from K to F as

$$N_{K/F}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(a).$$

(a) Suppose K/F is cyclic with Galois group $\mathbb{Z}/n\mathbb{Z}$ generated by σ. For any $\alpha \in K$ with $N_{K/F}(\alpha) = 1$, prove there exists $\beta \in K^\times$ such that $\alpha = \beta/\sigma(\beta)$. Suggested strategy: use linear independence of characters to show there exists $\theta \in K$ such that

$$\beta = \theta + \alpha\sigma(\theta) + (\alpha\sigma(\alpha))\sigma^2(\theta) + \cdots + (\alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha))\sigma^{n-1}(\theta) \neq 0.$$

(This can be interpreted as a statement about the group cohomology of the cyclic group.)

Proof. The linear independence of the characters $\sigma^i|_{K^\times} : K^\times \to K^\times$ ensures that $\sum_{i=0}^{n-1} a_i\sigma^i$ is not the zero function if and only if some a_j is nonzero. Observe that in $\mathrm{id}_{K^*}(\cdot) + \alpha\sigma(\cdot) + (\alpha\sigma(\alpha))\sigma^2(\cdot) + \cdots + (\alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha))\sigma^{n-1}(\cdot)$, none of the coefficients are zero since $N_{K/F}(\alpha) = 1$ by assumption. Hence this function is not the zero function so that there exists θ with

$$\theta + \alpha\sigma(\theta) + (\alpha\sigma(\alpha))\sigma^2(\theta) + \cdots + (\alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha))\sigma^{n-1}(\theta) = \beta \neq 0.$$

Observe that

$$\sigma(\beta) = \sigma(\theta) + \sigma(\alpha)\sigma^2(\theta) + (\sigma(\alpha)\sigma^2(\alpha))\sigma^3(\theta) + \cdots + (\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha))\theta \neq 0.$$

Then since $N_{K/F}(\alpha) = \sigma(\alpha)\sigma^2(\alpha)\cdots\alpha = 1$, we have that $\alpha\cdot\sigma(\beta) = \beta$ so that $\alpha = \beta/\sigma(\beta)$ as desired. □

(b) Prove that solutions $a, b \in \mathbb{Q}$ of Pythagoras's equation $a^2 + b^2 = 1$ are of the form

$$a = \frac{s^2 - t^2}{s^2 + t^2} \quad b = \frac{2st}{s^2 + t^2}$$

for some $s, t \in \mathbb{Q}$. Clear denominators and conclude that every right triangle whose three side lengths are relatively prime integers has side lengths $m^2 - n^2, 2mn$, and $m^2 + n^2$ for some $m, n \in \mathbb{Z}$. Suggested strategy: $a^2 + b^2$ is the norm of $a + bi$ in $\mathbb{Q}(i)$.

Proof. Observe that $\mathbb{Q}(i)$ is a Galois extension of $\mathbb{Q}$ of degree 2, so the only nontrivial automorphism of $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ is the conjugation map. Then $(a + bi)(a - bi) = a^2 + b^2$ is the norm from $\mathbb{Q}(i)$ to $\mathbb{Q}$.

Thus for rational complex numbers z with $|z| = 1$, it follows from Hilbert's theorem 90 that there exists a rational complex number $\beta = s + it \neq 0$ such that $z = \beta/\overline{\beta}$. Rationalizing, we have $z = \frac{s^2-t^2}{s^2+t^2} + i\frac{2st}{s^2+t^2}$; which proves the first result.

Clearing denominators via α, we obtain the integer complex number αz. Geometrically its real and imaginary parts determine the legs to a right triangle, and the hypotenuse is given by αz itself. The side lengths are relatively prime integers (we started with a rational complex number in reduced form), and they are of the form $m^2 - n^2, 2mn$, and $m^2 + n^2$ for some $m, n \in \mathbb{Z}$ (these are the lengths obtained after scaling $s^2 - t^2, 2st$, and $s^2 + t^2$ by α). □

Feedback

1. None.

2. This teaching style is much different than what I am used to – Usually the lectures are more blocky with clear cut lines between when we prove lemmas/theorems/other results, and the professor doesn't ask the students questions often. I like the way you're doing the lectures because they feel more "conversational" perhaps; they flow a bit more to me (this might also be due to the assigned reading). I like having the ability to talk to my neighbors when you ask questions, since they might have clever ideas that I didn't think of, and I like having someone make sure my reasoning makes sense too. I think one thing that would make me learn better is to kind of summarize what we achieved in class in maybe a sentence so I could leave with something like that on my mind before I start reading again (this is definitely something I could do myself too but maybe it would help others). This to me improves the flow between each class since in between class I have a nice way to summarize what I've learned. I think it's okay to leave things for the textbook as a reference since I find myself reading the results in it many times over during working on the homework, but maybe this isn't the case with others. Overall, I am feeling very fine about the way class is going and I would feel just fine if it stayed the way it has been.