HW5f

Math 172: Galois Theory

Jun 14 at 1:00

Prof. Thonkers

Stephen Xu

Problem 1

24.1.17

Let $F \subseteq E$ be a field extension. Assume that $f, g \in F[x]$ are distinct, monic, and irreducible. Show that f and g cannot have a common root in E.

We know that f and g will not have a common root in E if they are relatively prime to one another in F. We know that they are distinct, monic and irreducible. Therefore, it's easy to see that they are relatively prime, so they do not share a common root in E. ❤️

Problem 2

24.1.19

Let $F \subseteq E$ with $|E : F| < \infty$. Suppose $f \in F[x]$ is irreducible and $\deg(f) = p$, a prime. If f reduces in $E[x]$, show that p divides $|E : F|$.

We know that E is a finite degree extension over F. Consider $E \subseteq L$, where L includes a root of f, α, such that $\alpha \in L$. Therefore we have that $|F[\alpha] : F| = p$.

$$|E[\alpha] : F| = |E[\alpha] : F[\alpha]| \; |F[\alpha] : F|$$

From this, we can see that p divides $|E[\alpha] : F|$

Now, lets consider $g = \min_E(\alpha)$. $f \in E[x]$ and α is a root of f, so we know that $g \mid f$ in $E[x]$. Because f is reducible in $E[x]$, then we have that $\deg(g) < \deg(f) = p$, so $p \nmid |E[\alpha] : E|$. Thus we have

$$|E[\alpha] : F| = |E[\alpha] : E| \; |E : F|$$

Because $p \mid |E[\alpha] : F|, p \nmid |E[\alpha] : E|$, then we know that p divides $|E : F|$. ❤️

Problem 3

24.2.10

Let $\mathbb{Q} \subseteq E \subseteq \mathbb{C}$. Assume E is the (unique) splitting field for $x^p - 2$ over $\mathbb{Q}$ inside $\mathbb{C}$, and assume that p is a prime number. Find $|E : \mathbb{Q}|$.

We know that the roots can be written as the real root, $\sqrt[p]{2}$ as well as a bunch of imaginary roots, $\zeta_p \sqrt[p]{2}$. We thus know that $E = \mathbb{Q}\left(\sqrt[p]{2}, \zeta_p\right)$. We thus are trying to find $|\mathbb{Q}\left(\zeta_p, \sqrt[p]{2}\right) : \mathbb{Q}|$.

$$|\mathbb{Q}\left(\zeta_p, \sqrt[p]{2}\right) : \mathbb{Q}| = |\mathbb{Q}\left(\zeta_p, \sqrt[p]{2}\right) : \mathbb{Q}\left(\sqrt[p]{2}\right)| \ |\mathbb{Q}\left(\zeta_p\right) : \mathbb{Q}|$$

We know that the p-th cylcotomic polynomial is the minimal polynomial for ζ_p, with degree $p - 1$. It's also easy to see that $x^p - 2$ is the minimal polynomial for $\sqrt[p]{2}$ over $\mathbb{Q}$. Therefore we have that

$$|\mathbb{Q}\left(\zeta_p, \sqrt[p]{2}\right) : \mathbb{Q}| = p(p - 1)$$

And we obtain our answer of $|E : \mathbb{Q}| = p(p - 1)$. ❤️

Problem 4

24.3.2

Find $G = \mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{7}, \sqrt{11}\right)/\mathbb{Q}\right)$. Give a complete argument for all your assertions. Choose a set S of generators for G and let Ω be the set of roots, in $\mathbb{Q}\left(\sqrt{7}, \sqrt{11}\right)$, of the polynomial $(x^2 - 7)(x^2 - 11)$. Draw the Cayley digraph of the action of G on Ω.

We know that the minimal polynomials for $\alpha = \sqrt{7}, \beta = \sqrt{11}$ are $x^2 - 7$ and $x^2 - 11$ respectively, over both $\mathbb{Q}$, $\mathbb{Q}\left(\sqrt{11}\right)$ or $\mathbb{Q}\left(\sqrt{7}\right)$ respectively. Let us also define $E = \mathbb{Q}\left(\sqrt{7}, \sqrt{11}\right)$.

Then we have

$$|E : \mathbb{Q}| = \left|E : \mathbb{Q}\left(\sqrt{7}\right)\right| \left|\mathbb{Q}\left(\sqrt{7}\right) : \mathbb{Q}\right| = 2 \times 2 = 4$$

Therefore E as a vector space has a basis of 4 elements over $\mathbb{Q}$. We can therefore write

$$E = \left\{a + b\sqrt{7} + c\sqrt{11} + d\sqrt{77} \mid a, b, c, d \in \mathbb{Q}\right\}$$

We also know E is the splitting field of $(x^2 - 7)(x^2 - 11)$ over $\mathbb{Q}$. We also know each element of $\mathrm{Gal}(E/\mathbb{Q})$ is determined by its action on $\sqrt{7}, \sqrt{11}$.

We know that $x^2 - 7$ is irreducible in $\mathbb{Q}$, so $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{7}\right)/\mathbb{Q}\right)$ acts transitively on $\left\{\sqrt{7}, -\sqrt{7}\right\}$. Therefore there are two $\mathbb{Q}$-automorphisms of $\mathbb{Q}\left(\sqrt{7}\right)$. One fixes $\sqrt{7}$, and the other performs an additive inverse. We can extend these two $\mathbb{Q}$-automorphisms into $\mathbb{Q}\left[\sqrt{7}, \sqrt{11}\right]$.

We apply this same process for $x^2 - 11$.

We thus have $\mathrm{Gal}(E/F) = \{e, \sigma, \tau, \sigma\tau\}$, where the maps are

$$\begin{aligned}
e &: a + b\sqrt{7} + c\sqrt{11} + d\sqrt{77} \mapsto a + b\sqrt{7} + c\sqrt{11} + d\sqrt{77} \\
\sigma &: a + b\sqrt{7} + c\sqrt{11} + d\sqrt{77} \mapsto a - b\sqrt{7} + c\sqrt{11} - d\sqrt{77} \\
\tau &: a + b\sqrt{7} + c\sqrt{11} + d\sqrt{77} \mapsto a + b\sqrt{7} - c\sqrt{11} - d\sqrt{77} \\
\sigma\tau &: a + b\sqrt{7} + c\sqrt{11} + d\sqrt{77} \mapsto a - b\sqrt{7} - c\sqrt{11} + d\sqrt{77}
\end{aligned}$$

Therefore we obtain that $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{7}, \sqrt{11}\right)/\mathbb{Q}\right) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. ❤️

Problem 5

24.3.5

Let $F \subseteq E$ be fields with $|E : F| < \infty$. Assume $E = F[\alpha]$. Show

$$|\mathrm{Gal}(E/F)| \leq |E : F|$$

If $E = F[\alpha]$, then every F-automorphism is based on what the action of $\mathrm{Gal}(E/F)$ does to α. Therefore, we can define $\Omega = \{\text{roots of } \min_F(\alpha) \in E\}$. We can define a homomorphism and show that it's one to one, $\varphi : \mathrm{Gal}(E/F) \to \Omega$ where $\varphi(\sigma) = \varphi(\alpha)$, and $\sigma \in E$.

We have $\sigma_1, \sigma_2 \in E$ such that $\varphi(\sigma_1) = \varphi(\sigma_2)$. We want to show that $\sigma_1 = \sigma_2$. We know that $\sigma_1(\alpha) = \sigma_2(\alpha)$. They both agree on α, and fix F. Therefore they are the same, so $\sigma_1 = \sigma_2$ and φ is 1-1. Thus,

$$|\mathrm{Gal}(E/F)| \leq |\Omega| \leq \deg(\min_F(\alpha)) = |E : F|$$

So we show that $|\mathrm{Gal}(E/F)| \leq |E : F|$. ❤️

Problem 6

24.3.7

Let $\alpha = \sqrt{2+\sqrt{2}} \in \mathbb{C}$.

a) Compute $f = \min_{\mathbb{Q}}(\alpha)$.

b) Find $E \subseteq \mathbb{C}$ such that E is the splitting field for f over $\mathbb{Q}$. Compute $|E : \mathbb{Q}|$.

c) Show that $\mathrm{Gal}(E/\mathbb{Q})$ contains an element of order 4.

a) Consider $\alpha^2 - \sqrt{2} = 2$. Rearranging, we obtain $\alpha^2 = 2 + \sqrt{2}$. We thus have $\alpha^4 = \left(2+\sqrt{2}\right)^2 \Rightarrow \alpha^4 - 4\sqrt{2} - 6 = 0$. We can rewrite $4\sqrt{2} + 6$ in terms of α^2, obtaining $4\sqrt{2} + 6 = 4\alpha^2 - 2$. Therefore $\alpha^4 - 4\alpha^2 + 2$. As such we obtain a potential minimal polynomial $x^4 - 4x^2 + 2$. Using Eisenstein's, we see it's irreducible and monic with α as a root. Therefore $f = x^4 - 4x^2 + 2$.

b) We can find the roots as $\pm\sqrt{2+\sqrt{2}}, \pm\sqrt{2-\sqrt{2}}$. We note that because they share the same minimal polymial, $|E : \mathbb{Q}| = \deg\left(\min_{\mathbb{Q}}(\alpha)\right) = 4$, and we have that $E = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}, \sqrt{2-\sqrt{2}}\right)$.

c) Consider the automorphism $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ such that $\varphi(\alpha) = \beta$, where $\beta = \sqrt{2-\sqrt{2}}$. Consider

$$\varphi\left(\sqrt{2}\right) = \varphi\left(\sqrt{\alpha\beta}\right) = \varphi(\alpha^2 - 2) = \varphi(\alpha)^2 - \varphi(2) = \beta^2 - 2 = -\sqrt{2}$$

Using this, we see that we can use σ recursively to obtain $\beta, \alpha, -\alpha, -\beta$. We thus show that σ is an element of order 4 in $\mathrm{Gal}(E/\mathbb{Q})$. ❤️