Graded

1. (14.4.6) Prove that $\mathbb{F}_p(x,y)/\mathbb{F}_p(x^p,y^p)$ is not a simple extension by explicitly exhibiting an infinite number of intermediate subfields.

   Proof. The extension $\mathbb{F}_p(x,y)/\mathbb{F}_p(x^p,y^p)$ is degree p^2 as the minimal polynomial for x is $t^p - x^p$ and the minimal polynomial for y is $t^p - y^p$, so the extension is degree p^2 by the tower law. We show that there are infinitely many distinct intermediate subfields which are degree p extensions of $F = \mathbb{F}_p(x^p,y^p)$.

   Consider the family of extensions $F(x+cy)/F$ for $c \in F$, which is infinite since F is infinite (as x, y are indeterminates). Each extension is degree p since the minimal polynomial for $x+cy$ is $t^p - (x+cy)^p$ and by Frobenius we have $(x+cy)^p = x^p + c^p y^p \in F$.

   If two extensions $F(x+cy)$ and $F(x+dy)$ were equivalent, then the difference $(c-d)y \in F(x+cy)$, and so also $x \in F(x+cy)$ so that $F(x,y) = \mathbb{F}_p(x,y) \subseteq F(x+cy)$. This is impossible by degree considerations, so it follows that any two extensions in the given family are distinct.

   Since there are infinitely many distinct intermediate subfields of the extension $\mathbb{F}_p(x,y)/\mathbb{F}_p(x^p,y^p)$, it cannot be simple. □

2. (14.5.7) Show that complex conjugation restricts to the automorphism $\sigma_{-1} \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ of the cyclotomic field of n^{th} roots of unity. Show that the field $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the subfield of real elements in $K = \mathbb{Q}(\zeta_n)$, called the *maximal real subfield of* K.

   Proof. Recall that complex conjugation respects sums and products so that for any rational function $P(\zeta_n)/Q(\zeta_n)$ of ζ_n over $\mathbb{Q}$, its complex conjugate is $P(\overline{\zeta_n})/Q(\overline{\zeta_n})$. But $\zeta_n = \exp(2\pi i/n)$ so that $\overline{\zeta_n} = \exp(-2\pi i/n) = \zeta_n^{-1}$. Furthermore, ζ_n^{-1} is also a primitive n-th root of unity since -1 is coprime with n. So complex conjugation restricted to $\mathbb{Q}(\zeta_n)$ agrees with the automorphism σ_{-1} which sends ζ_n to ζ_n^{-1}.

   Observe that elements fixed by complex conjugation are real and conversely. We find the fixed field of the subgroup generated by $\{\sigma_{-1}\}$ and show it is K^+ as above. Observe that elements of K^+ are rational functions of $\zeta_n + \zeta_n^{-1}$, and so σ_{-1} fixes these rational functions since $\sigma_{-1}(\zeta_n + \zeta_n^{-1}) = \zeta_n^{-1} + \zeta_n$ and σ_{-1} fixes real elements. Hence K^+ is contained in the fixed field.

   The degree of K over K^+ is 2: The monic polynomial $x^2 - (\zeta_n + \zeta_n^{-1})x + 1$ is irreducible since its roots ζ_n, ζ_n^{-1} are complex, so it is the minimal polynomial for ζ_n over K^+. The extension $K/\mathbb{Q}$ is Galois with Abelian Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$ (so every intermediate subfield is Galois over $\mathbb{Q}$), which has order $\phi(n)$. The degree of the fixed field K^H of $H = \{1, \sigma_{-1}\} \cong \mathbb{Z}/2\mathbb{Z}$ over $\mathbb{Q}$ must be $\phi(n)/2$ by the Galois correspondence. Hence the degree of K over K^H is 2 also.

   But the fixed field contains K^+ as a subfield, and K^H is a proper subfield of K (as K contains complex elements while K^H only contains real elements). Since 2 is prime it follows that $[K^H : K^+] = 1$. Hence K^+ is the fixed field of H, the maximal real subfield of K. □

Additional Problems

1. (14.4.1) Determine the Galois closure of the field $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ over $\mathbb{Q}$.

   Proof. We show that the Galois closure of $F = \mathbb{Q}(\sqrt{1+\sqrt{2}})$ is $K = \mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}})$, the splitting field of the separable polynomial $p(x) = x^4 - 2x^2 - 1$ (with roots are $\pm\sqrt{1 \pm \sqrt{2}}$). We first show that $p(x)$ is irreducible so that it is the minimal polynomial of $\sqrt{1+\sqrt{2}}$: The extension F over $\mathbb{Q}(\sqrt{2})$ is degree 2: consider the polynomial $x^2 - 1 - \sqrt{2}$. We show that $\alpha = \sqrt{1+\sqrt{2}}$ is not a square in $\mathbb{Q}(\sqrt{2})$ to show that the polynomial is irreducible. Suppose α is a square of an element $c = a + b\sqrt{2} \in \mathbb{Q}$. Then $a^2 + 2b^2 = -1$ and $2ab = -1$, so b is determined by a. We show that a could not be rational to obtain the contradiction. With $b = -1/2a$ we find with some algebra that a needs to satisfy $2a^4 + 2a^2 + 1 = 0$. By the rational root theorem a could not be rational so by contradiction α is not a square of an element of $\mathbb{Q}(\sqrt{2})$, so the polynomial $x^2 - 1 - \sqrt{2}$ is irreducible hence the minimal polynomial of $\sqrt{1+\sqrt{2}}$ over $\mathbb{Q}(\sqrt{2})$. It follows by the tower law that the degree of F over $\mathbb{Q}$ is 4, and since $\sqrt{1+\sqrt{2}}$ satisfied the degree 4 polynomial $p(x)$ over $\mathbb{Q}$, it follows that $p(x)$ was irreducible. Hence $p(x)$ is the minimal polynomial of $\sqrt{1+\sqrt{2}}$ over $\mathbb{Q}$.

   Then consider any other Galois extension L over $\mathbb{Q}$ containing F. We show that K is contained in L. Any irreducible polynomial with a root in L splits completely over L; in particular since L contains F the minimal polynomial $p(x)$ of $\sqrt{1+\sqrt{2}}$ splits completely, so L contains K. Since L was arbitrary it follows that K is the smallest Galois extension of $\mathbb{Q}$ containing F, the Galois closure of F as desired. □

   The other two I could have done but I got home too late.

2. (14.5.10) Prove that $\mathbb{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic field over $\mathbb{Q}$.

   Proof. Cyclotomic field extensions have Abelian Galois groups, so every intermediate subfield is Galois over $\mathbb{Q}$. But we saw earlier that $\mathbb{Q}(\sqrt[3]{2})$ is not Galois over $\mathbb{Q}$ so it could not be a subfield of a cyclotomic field extension. □

Feedback

1. None.
2. Things are okay so far; same as usual I think.