Algebra Homework 5

Due Wednesday, February 27

1

(a) Assume F has characteristic $p \neq 0$, and let $a \in F$. Show that $f = X^p - a$ either splits or is irreducible in $F[X]$.

(b) Let $F \subseteq \mathbb{C}$, and let $\epsilon = e^{2\pi i/p} \in F$, where p is a prime. Let $a \in F$. Show that $f = X^p - a$ either splits or is irreducible in $F[X]$.

Solution

(a) Let $E \supseteq F$ be a splitting field for f, and let $\alpha \in E$ be a root of f. Then we have $\alpha^p = a$, so

$$f = X^p - a = X^p - \alpha^p = (X - \alpha)^p.$$

Let $f = g_1 \cdots g_k$ be a factorization of f in $F[X]$ into monic irreducible factors. Each g_i is irreducible, monic, and has α as a root. Thus, each $g_i = m_{F,\alpha}$, so $\deg(m_{F,\alpha})$ divides p. This shows that either $f = m_{F,\alpha}$ or each $m_{F,\alpha} = X - \alpha$. In the first case, f is irreducible over F; in the second case, $\alpha \in F$, so f splits over F.

(b) Let $\alpha \in \mathbb{C}$ be a root of f in E and define $E = \mathbb{Q}[\alpha, \epsilon]$. Since each root of f has the form $\epsilon^k \alpha$, f splits over E. Furthermore, $|E : \mathbb{Q}[\epsilon]| = p$ (following Problem 3 of Assignment 1). Now consider the extension $E \supseteq E \cap F$. Since f is monic and has all its roots in E, $f \in E[X]$; but $f \in F[X]$ too, so $f \in (E \cap F)[X]$. Therefore E is a splitting field for a separable polynomial f over $E \cap F$, E is Galois over $E \cap F$. By Natural Irrationalities

$$|F[\alpha] : F| = |\langle F, E\rangle : F| = |E : E \cap F|$$

which divides $|E : \mathbb{Q}[\epsilon]| = p$. If $|E : E \cap F| = 1$, then $E \subseteq F$ and f splits over F. Otherwise, $\deg(m_{F,\alpha}) = |F[\alpha] : F| = p$, so f is irreducible.

2 Let $\alpha = \sqrt{3} + \sqrt[3]{2} \in \mathbb{C}$.

(a) Show that α is a primitive element for the extension $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3}, \sqrt[3]{2}]$

(b) Find a polynomial of degree 6 in $\mathbb{Q}[x]$ that has α as a root, and deduce that it must be irreducible.

Solution

We'll find our polynomial first. To do this, we calculate by the sweat of our brow:

$$\begin{aligned}
\alpha &= \sqrt{3} + \sqrt[3]{2} \\
\alpha - \sqrt{3} &= \sqrt[3]{2} \\
(\alpha - \sqrt{3})^3 &= 2 \\
\alpha^3 - 3\alpha^2\sqrt{3} + 9\alpha - 3\sqrt{3} &= 2 \\
\sqrt{3} &= \tfrac{\alpha^3+9\alpha-2}{3\alpha^2+3} \\
3(3\alpha^2+3)^2 &= (\alpha^3 + 9\alpha - 2)^2 \\
\alpha^6 - 9\alpha^4 - 4\alpha^3 + 27\alpha^2 - 36\alpha - 23 &= 0.
\end{aligned}$$

Notice that the fifth line shows that $\sqrt{3} \in \mathbb{Q}[\alpha]$, which shows that $\sqrt[3]{2} = \alpha - \sqrt{3} \in \mathbb{Q}[\alpha]$, and consequently, that $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{3}, \sqrt[3]{2}]$. Now observe that since $\mathbb{Q}[\sqrt{3}] \subseteq \mathbb{Q}[\sqrt{3}, \sqrt[3]{2}]$ and $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{Q}[\sqrt{3}, \sqrt[3]{2}]$, $|\mathbb{Q}[\sqrt{3}, \sqrt[3]{2}] : \mathbb{Q}| \geq 6$. On the other hand, $m_{\mathbb{Q}[\sqrt[3]{2}],\sqrt{3}}$ divides $X^2 - 3$, so

$$|\mathbb{Q}[\sqrt{3}, \sqrt[3]{2}] : \mathbb{Q}| = |\mathbb{Q}[\sqrt{3}, \sqrt[3]{2}] : \mathbb{Q}[\sqrt[3]{2}]| \cdot |\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}| \leq 2 \cdot 3 = 6.$$

This proves that $|\mathbb{Q}[\sqrt{3}, \sqrt[3]{2}] : \mathbb{Q}| = 6$, so $\deg(m_{\mathbb{Q},\alpha}) = 6$. We conclude that

$$m_{\mathbb{Q},\alpha} = X^6 - 9X^4 - 4X^3 + 27X^2 - 36X - 23,$$

and so this polynomial is irreducible. Notice that Eisenstein's criterion can't be applied to this polynomial (at least, not directly).

3 Let $F < E$ and suppose that $E = F[\alpha]$. Assume that $\alpha^p \in F$, where p is a prime number not equal to the characteristic of F. Show that the following are equivalent.

(a) F contains a primitive p^{th} root of unity;

(b) $|E : F| = p$ and E is Galois over F.

Solution

(a)⇒(b) Let $a = \alpha^p$, and $f = X^p - a$. Let $\epsilon \in F$ be a primitive p^{th} root of unity. Then $\{\alpha, \alpha\epsilon, \ldots, \alpha\epsilon^{p-1}\}$ is the set of all roots of f. This shows that f is a separable polynomial, and that $E = F[\alpha]$ is a splitting field for f over F. Hence E is Galois over F. Write $G = \mathrm{Gal}(E/F)$. Since $|G| = |E : F| > 1$, there is a nontrivial element $\sigma \in G$. Now $\sigma(\alpha) = \alpha\epsilon^i$ for some $0 < i < p$. Then $\sigma^p(\alpha) = \alpha$. Since σ is determined by its action on α, this shows that $\sigma^p = 1$. Hence $|G| \geq p$. On the other hand

$$|G| = |F[\alpha] : F| = \deg(m_{F,\alpha}) \leq p$$

because $m_{F,\alpha}$ divides f.

(b)⇒(a) Since $|F[\alpha] : F| = p$, $f = m_{F,\alpha}$. Since E is Galois over F, f has distinct roots and splits over E. Let $\beta \neq \alpha \in E$ be another root of f. Then $\epsilon = \frac{\alpha}{\beta}$ is a primitive p^{th} root of unity. Suppose $\epsilon \notin F$. Then $F \subseteq F[\epsilon]$ is a proper extension; and since $|F[\epsilon] : F|$ divides $|E : F| = p$, $E = F[\epsilon]$. This shows that $m_{F,\epsilon} = X^p - 1$. But this is impossible, because $(X - 1)$ divides $X^p - 1$.

4 Assume the situation of Problem 3 with $p \neq 2$, and assume that a and b both hold. Prove that α has no p^{th} root in E.

Solution

Assume $\beta \in E$ with $\beta^p = \alpha$. Let $\sigma \in G = \mathrm{Gal}(E/F)$ be a generator. Let $\delta = \frac{\sigma(\beta)}{\beta}$. Then $\delta^p = \frac{\sigma(\beta^p)}{\beta^p} = \frac{\sigma(\alpha)}{\alpha}$. Since σ is determined by its value on α, $\frac{\sigma(\alpha)}{\alpha} \neq 1$. Therefore $\delta^{p^2} = \frac{\sigma(\alpha^p)}{\alpha^p} = 1$ since $\alpha^p \in F$. Thus δ^p is a p^{th} root of 1, which means that $\delta^p \in F$. Let $\epsilon = \frac{\sigma(\delta)}{\delta}$. Then $\epsilon^p = 1$, using the fact that $\delta^p \in F$. Thus, $\epsilon \in F$.

To prove the formula, observe that it is true when $k = 0$. Now assume that it holds for k and prove it for $k + 1$. This is just a calculation

$$\sigma^{k+1}(\beta) = \sigma(\sigma^k(\beta)) = \sigma(\beta)\sigma(\delta^k)\epsilon^{k(k-1)/2}$$

the last step uses the fact that $\epsilon \in F$. Now from the definition of δ, $\sigma(\beta) = \delta\beta$; similarly, $\sigma(\delta) = \epsilon$. Thus

$$\sigma^{k+1}(\beta) = \delta\beta(\epsilon\delta)^k\epsilon^{k(k-1)/2} = \beta\delta^{k+1}\epsilon^{k(k+1)/2}$$

which is what we wanted to prove.

Set $k = p$ in the formula. This yields $\beta = \sigma^p(\beta) = \beta\delta^p\epsilon^{p(p-1)/2}$. Since $p \neq 2$, $(p-1)$ is even, so $\epsilon^{p(p-1)/2} = (\epsilon^p)^{(p-1)/2} = 1$. Thus, $\beta = \beta\delta^p$, so $\delta^p = 1$. But $\delta^p = \frac{\sigma(\alpha)}{\alpha}$, which shows that $\sigma(\alpha) = \alpha$, so $\sigma = 1$, which contradicts our assumption that σ was the generator of the nontrivial group G.