Algebra Homework 2

Due Monday, January 21

1 Let $F \subseteq E$, $f \in F[X]$ with $\deg(f) = n$, and assume that f splits over E. Show that there is a field L such that $F \subseteq L \subseteq E$ such that f splits over L and $|L : F| \leq n!$.

Solution

Let $\alpha_1, \ldots, \alpha_k$ be the roots of f; notice that $k \leq n$. Write $L_0 = F$, and for $i \leq k$, define $L_i = L_{i-1}[\alpha_i]$. Then

$$|L_i : L_{i-1}| = \deg(m_{L_{i-1},\alpha_i}).$$

Let $L = L_k$. This means that

$$|L : F| = \prod_{i=1}^{k} |L_i : L_{i-1}|.$$

Because $\alpha_1, \ldots, \alpha_{i-1} \in L_{i-1}$, $f/(X - \alpha_1) \cdots (X - \alpha_{i-1}) \in L_{i-1}[X]$. Therefore

$$|L_i : L_{i-1}| = \deg(m_{L_{i-1},\alpha_i}) \leq n - i + 1$$

and this finishes the proof.

2 Let $\alpha, \beta \in \mathbf{C}$ be distinct roots of $f = X^p - 2$, where p is a prime number.

a Show that f splits over $\mathbf{Q}[\alpha, \beta]$.

b Let $\epsilon = \alpha/\beta$. Compute $|\mathbf{Q}[\epsilon] : \mathbf{Q}|$. (**Hint:** What is $m_{\mathbf{Q},\epsilon}$?)

c Compute $|\mathbf{Q}[\alpha, \beta] : \mathbf{Q}|$.

(**Hint:** $X^{p-1} + X^{p-2} + \cdots + 1$ is irreducible.)

Solution

a Let $\epsilon = \alpha/\beta$. Then $\epsilon^p = 1$; because $\alpha \neq \beta$, $\epsilon \neq 1$, so $\{1, \epsilon, \ldots, \epsilon^{p-1}\}$ are all the roots of X^{p-1}. Therefore $\{\alpha, \alpha\epsilon, \ldots, \alpha\epsilon^{p-1}\}$ are all the roots of $X^p - 2$.

b We have seen that ϵ is a root of

$$(X^p - 1)/(X - 1) = X^{p-1} + X^{p-2} + \cdots + 1,$$

which is irreducible, hence the minimal polynomial of ϵ. Thus, $|\mathbf{Q}[\epsilon] : \mathbf{Q}| = \deg(X^{p-1} + X^{p-2} + \cdots + 1) = p - 1$.

c We have

$$\mathbf{Q} \subseteq \mathbf{Q}[\epsilon] \subseteq \mathbf{Q}[\alpha, \beta]$$

which shows that $(p - 1)$ divides $|\mathbf{Q}[\alpha, \beta] : \mathbf{Q}|$. By the Eisenstein criterion $X^p - 2$ is irreducible, which means that $|\mathbf{Q}[\alpha] : \mathbf{Q}| = p$, and the chain

$$\mathbf{Q} \subseteq \mathbf{Q}[\alpha] \subseteq \mathbf{Q}[\alpha, \beta]$$

shows that $|\mathbf{Q}[\alpha, \beta] : \mathbf{Q}|$ is divisible by p. Thus, $|\mathbf{Q}[\alpha, \beta] : \mathbf{Q}| \geq p(p-1)$. On the other hand,

$$\mathbf{Q} \subseteq \mathbf{Q}[\alpha] \subseteq \mathbf{Q}[\alpha, \epsilon] = \mathbf{Q}[\alpha, \beta]$$

and $|\mathbf{Q}[\alpha, \epsilon] : \mathbf{Q}[\alpha]| \leq p - 1$, so $|\mathbf{Q}[\alpha, \beta] : \mathbf{Q}| \leq p(p - 1)$.

3 Let $f \in F[X]$ with $\deg(f) = p$, a prime number. Assume that f is irreducible in $F[X]$. Let $F \subseteq E$ be a finite degree extension, and assume that f is *not* irreducible over E (but not necessarily that f has a root in E). Show that p divides $|E : F|$. (**Hint:** Choose a field $L \supseteq E$ in which f has a root α, and think about $|E[\alpha] : F|$.)

Solution

Let L be an extension of E in which f has a root, α, and look at $E[\alpha]$, which has finite degree over E, and hence has finite degree over F. We have

$$F \subseteq F[\alpha] \subseteq E[\alpha].$$

and $|F[\alpha] : F| = p$, so p divides $|E[\alpha] : F| = |E[\alpha] : E|\,|E : F|$. Since f splits over E, $\deg(m_{E,\alpha}) < p$, so p does not divide $|E[\alpha] : E|$. This forces p to divide $|E : F|$.

4 Let $\alpha = \sqrt{2+\sqrt{2}} \in \mathbf{R}$.

a Determine the minimal polynomial $f = m_{\mathbf{Q},\alpha}$.

b Show that f splits over $E = \mathbf{Q}[\alpha]$.

c Show that $\mathrm{Gal}(E/F)$ contains an element of order 4 (note: $F = \mathbf{Q}$).

Solution

a Let $f(X) = (X^2-2)^2 - 2 = X^4 - 4X^2 + 2$. Then $f(\alpha) = 0$, and f is irreducible over $\mathbf{Q}$ by the Eisenstein criterion. Thus $f = m_{\mathbf{Q},\alpha}$.

b Let $\beta = \sqrt{2-\sqrt{2}}$, so the roots of f are precisely $\pm\alpha$ and $\pm\beta$. We have to show that $\beta \in \mathbf{Q}[\alpha]$. Since $\alpha\beta = \sqrt{2}$, and $\sqrt{2} = \alpha^2 - 2$,

$$\beta = (\alpha^2 - 2)/\alpha \in \mathbf{Q}[\alpha].$$

c Since E is a splitting field for a separable polynomial over $\mathbf{Q}$, $\mathrm{Gal}(E/F)$ permutes the 4 roots of f transitively. Let $\sigma \in \mathrm{Gal}(E/F)$ be such that $\sigma(\alpha) = \beta$. Then $\sigma^2(\alpha) = -\alpha$ and $\sigma^4(\alpha) = \alpha$. Thus $\sigma^4 = 1_E$, and so σ has order 4.