Algebra HW 4

Zack Garza

① Since F is algebraically closed over K, every $f(x) \in F[x]$ has a root in F. Since we want to show that E is also algebraically closed, let $f(x) \in E[x]$; we will show f has a root in E. Writing $f(x) = \sum_{i=0}^{n} e_i x^i$, consider $J := K(e_1, \cdots, e_n)$; then $f \in J[x]$. We have $[J:K] = n < \infty$, and since $K \leq J \leq E \leq F \Rightarrow K[x] \leq J[x] \leq E[x] \leq F[x]$, we have $f \in F[x]$ and so f has a root $\alpha \in F$. But $[J(\alpha) : J] < \infty$, and thus $[J(\alpha) : k] = [J(\alpha) : J][J : k] < \infty$, so α is algebraic over k. Then $\alpha \in E$ by defn. But then E is <u>an algebraic extension of k that is algebraically closed</u>, so E is an algebraic closure of k. $\blacksquare$

---

2) Suppose $K = \{k_1, \cdots, k_n\}$ is finite, and consider $f(x) = \overset{\neq 0 \in k}{k_1} + \prod_{i=1}^{n} (x - k_i) \in K[x]$. Then

$f(k_i) = k_i \neq 0$, so f has no root in K. Thus $K \neq \overline{K}$. $\blacksquare$

---

3) Let p be prime; for any group G we have $g \in G \Rightarrow g^{|G|} = e$. Since $\mathbb{Z}_p$ is a field, $(\mathbb{Z}_p^\times, \times)$ is a group. In particular, $|\mathbb{Z}_p^\times| = p-1$, so for every $x \in \mathbb{Z}_p^\times$ we have $x^{p-1} = 1$. Multiplying by x yields $x^p = x$ (since no element of $\mathbb{Z}_p^\times$ is a zero divisor.) Since this also holds for $x = 0$ in $\mathbb{Z}_p$, it thus holds for all $x \in \mathbb{Z}_p$. $\blacksquare$

---

4) Let $|K| = p^n$ and consider the Frobenius endomorphism $\phi : K \to K,\ x \mapsto x^p$

This is a field homomorphism since $\mathrm{char}(K) = p$, which yields

$$\phi(x+y) = (x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i = x^p + y^p = \phi(x) + \phi(y).$$

p divides all but first/last terms

We have $\ker \phi = \phi^{-1}(0) = \{x \in K \mid x^p = 0\} = 0$, since no element of a field can be nilpotent (otherwise $x \cdot x^{p-1} = 0 \Rightarrow x$ is a zero divisor $\Rightarrow x$ is not a unit). But then ϕ is an injective endomorphism and thus bijective since $|\mathrm{domain}(\phi)| = |\mathrm{range}(\phi)| < \infty$. Thus for every $x \in k$, $\phi^{-1}(x)$ is a unique p^{th} root of x. $\blacksquare$

---

5) Suppose K is a field, then $|K|=p^n$ and $\text{char}(K)=p$. If $p=2$, then $\phi: \begin{array}{l} K \to K \\ x \mapsto x^2 \end{array}$ is an automorphism and thus we can write any $x \in K$ as $x = \phi^{-1}(x)^2 + 0^2$.

Otherwise, p is odd, so $|K^\times| = p^n - 1$ is even, so $p^n - 1 = 2\ell$ for some $\ell \in \mathbb{N}^{>0}$. Moreover, $K^\times$ is cyclic, say $K^\times = \langle \alpha \rangle$, where $\text{order}(\alpha) = p^n - 1 = 2\ell$, so

$$\alpha^{2m} = (\alpha^m)^2 = \beta \neq 1 \text{ for each } m \text{ s.t. } 1 \leq m < \ell,$$

so this yields $\ell = p^n - 1/2$ elts that are the squares of some elements in $K^\times \subseteq K$. <u>Now fix some $x \in K^\times$</u>, and consider the sets

$$P = \{(\alpha^m)^2 \mid 1 \leq m < \ell\} \cup \{0\} \text{ and } Q = \{x - p \mid p \in P\}$$

We have $|P| = |Q| = \frac{1}{2}(p^n - 1) + 1$, so

$$|Q| + |P| = p^n + 1 > |K|.$$

So $Q \cap P$ is nonempty, but then $\beta \in Q \cap P \Rightarrow \beta = (\alpha^m)^2 = x - (\alpha^n)^2$ for some m, n, so

$$x = (\alpha^m)^2 + (\alpha^n)^2$$

as desired. ∎

---

6) Since $\gcd(p,n) = 1$, write $1 = tp + sn$ for some $t, s \in \mathbb{Z}$. Then

$$v \in F \Rightarrow v = (tp + sn)v = tpv + snv \in F.$$

Since $\text{char}\, K = p$, $tpv = 0$, so $v = s(nv)$.

Since $nv \in K$, $s(nv) \in K$, and so $v \in K$ must hold as well. ∎

---

7) Let $n = [F:K] < \infty$ where $p \nmid n$. Let $\alpha \in F$ and $f(x) = \min(\alpha, F) \in K[x] \subseteq F[x]$; we will show that f has no repeated roots. We have $d = \deg f = [K(\alpha):K]$, and thus $f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_1 x + c_0$. But $n = [F:K] = [F:K(\alpha)][K(\alpha):K] = m \cdot d$, and since $p \nmid n$, we have $p \nmid d$, so we can compute $f'(x) = dx^{d-1} + \cdots c_1$, and the leading coefficient is <u>nonzero</u>. So $\deg f' = d-1 < \deg f = d$. Moreover, $f'(x)$ is not the zero polynomial. Since f was irreducible in $F[x]$, we can only possibly have $\gcd(f, f') \in \{1, f(x)\}$ - but $\gcd(f, f') = f$ would imply $f(x) \mid f'(x)$, contradicting $\deg f < \deg f'$. So $\gcd(f, f') = 1$, which happens iff $f(x)$ has no repeated roots. ∎
