Solutions to Homework 9 **Math 5591H**

A1. *Let L/F be an extension and let $f \in F[x]$.*

5pt (a) *If K is a spitting field of f over F and $K \supseteq L$, prove that K is a splitting field of f over L.*

Solution. f splits completely in K (this doesn't depend on whether we consider f as an element pf $F[x]$ or $L[x]$). Also, K is a minimal such field containing F, so it is a minimal such field containing L.

5pt (b) *Give an example where K is a splitting field of f over L, but is not a splitting field of f over F.*

Solution. $\mathbb{Q}(i, \sqrt{2})$ is a spltting field of $x^2 - 2$ over $\mathbb{Q}(i)$ but not over $\mathbb{Q}$.

A2. *Let F be a field of characteristic p and let $f \in F[x]$ be irreducible.*

5pt (a) *Prove that $f(x) = g(x^{p^k})$ for some separable irreducible $g \in F[x]$ and some integer $k \geq 0$.*

Solution. If f is separable, we put $g = f$. If f is inseparable, then, as we know, $f(x) = h(x^p)$ for some $h \in F[x]$. h is irreducible since if h is reducible, $h = h_1 h_2$, then $f(x) h_1(x^p) h_2(x^p)$ is reducible either. Since $\deg h < \deg f$, by induction on $\deg f$, $h(x) = g\big(x^{p^l}\big)$ for some irreducible $g \in F[x]$. Then $f(x) = g\big(x^{p^{l+1}}\big)$.

5pt (b) *Prove that in its splitting field, $f(x) = c(x - \alpha_1)^{p^k} \cdots (x - \alpha_d)^{p^k}$ for some distinct $\alpha_1, \ldots, \alpha_d$.*

Solution. We may assume that f is monic. Let $f(x) = g(x^{p^k})$ where g is separable. Let $\beta_1, \ldots, \beta_d$ be the (distinct) roots of g (in its splitting field), so that $g(x) = (x - \beta_1) \cdots (x - \beta_d)$ and $f(x) = g(x^{p^k}) = (x^{p^k} - \beta_1) \cdots (x^{p^k} - \beta_d)$. For every i, let α_i be a root of $x^{p^k} - \beta_i$; then $(x - \alpha_i)^{p^k} = x^{p^k} - \alpha_i^{p^k} = x^{p^k} - \beta_i$. So, $f(x) = (x - \alpha_1)^{p^k} \cdots (x - \alpha_d)^{p^k}$.

10pt **13.5.5.** *Let p be a prime integer, let $a \in \mathbb{F}_p$, $a \neq 0$, and let $f = x^p - x + a \in \mathbb{F}_p[x]$. Prove that the splitting field K of f is obtained by adjoining a single root of f. Prove that f is separable and irreducible over $\mathbb{F}_p$.*

Solution. $f' = -1$, so f' has no roots, so f has no common roots with f', and so, f has no multiple roots. Hence, f is separable.

f has no roots in $\mathbb{F}_p$, since for any $b \in \mathbb{F}_p$, $b^p = b \neq b - a$. Let α be a root of f (in an extension of $\mathbb{F}_p$), so that $\alpha^p = \alpha - a$. Then for any $b \in \mathbb{F}_p$ we have $(\alpha + b)^p = \alpha^p + b^p = \alpha - a + b = (\alpha + b) - a$, so $\alpha + b$ is also a root of f. (Hence, f has p distinct roots, $\alpha + b$ for all $b \in \mathbb{F}_p$, so, we see again that f is separable.) It follows that $K = \mathbb{F}_p(\alpha)$ is a splitting field of f.

Let's now prove that f is irreducible. Since $\alpha \notin \mathbb{F}_p$, it has at least one conjugate, $\alpha + b$ for some nonzero $b \in \mathbb{F}_p$. There is an isomorphism $\varphi \colon K \longrightarrow K$ over $\mathbb{F}_p$ that maps α to $\alpha + b$. Since α and $\alpha + b$ are conjugate, the elements $\varphi(\alpha) = \alpha + b$ and $\varphi(\alpha + b) = \alpha + 2b$ are conjugate, and so, α and $\alpha + 2b$ are conjugate. Thus, by induction, all the roots $\alpha + kb$, $k = 0, 1, \ldots, p - 1$, of f are conjugate, so f is irreducible.

10pt **A3.** (a) *Let $n = p^r m$ where p is prime and $p \nmid m$. Prove that $\Phi_n(x) = \Phi_{pm}(x^{p^{r-1}})$.*

Solution.

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(x)} = \frac{x^{p^r m} - 1}{\prod_{d|p^{r-1}m} \Phi_d(x) \prod_{\substack{d|m \\ d<m}} \Phi_{dp^r}(x)}.$$

We have $x^{p^r m} - 1 = (x^{p^{r-1}})^{pm} - 1$, $\prod_{d|p^{r-1}m} \Phi_d(x) = x^{p^{r-1}m} - 1 = (x^{p^{r-1}})^m - 1 = \prod_{d|m} \Phi_d(x^{p^{r-1}})$, and by induction, for any $d < m$, $\Phi_{dp^r}(x) = \Phi_{dp}(x^{p^{r-1}})$. So,

$$\Phi_n(x) = \frac{(x^{p^{r-1}})^{pm} - 1}{\prod_{d|m} \Phi_d(x^{p^{r-1}}) \prod_{\substack{d|m \\ d<m}} \Phi_{dp}(x^{p^{r-1}})} = \Phi_{pm}(x^{p^{r-1}}).$$

Another solution. The polynomials $\Phi_n(x)$ and $\Phi_{pm}(x^{p^{r-1}})$ have the same degree, $\varphi(n) = \varphi(p^r)\varphi(m) = p^{r-1}(p-1)\varphi(m) = p^{r-1}\varphi(p)\varphi(m) = p^{r-1}\varphi(pm)$. Also, if ω is a root of Φ_n, that is, a primitive root of 1 of degree n, then $\omega^{p^{r-1}}$ is a primitive root of 1 of degree pm, so ω is a root of $\Phi_{pm}(x^{p^{r-1}})$. Since Φ_n is separable, this implies that $\Phi_n(x)$ divides $\Phi_{pm}(x^{p^{r-1}})$, and so, these polynomials are equal.

5pt (b) *Deduce that if $n = p_1^{r_1} \cdots p_k^{r_k}$ is the prime factorization of n, then $\Phi_n(x) = \Phi_d(x^q)$, where $d = p_1 \cdots p_k$ and $q = p_1^{r_1 - 1} \cdots p_k^{r_k - 1}$.*

Solution. Applying (a) k times, we get

$$\Phi_n(x) = \Phi_{p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}}(x) = \Phi_{p_1 p_2^{r_2} \cdots p_k^{r_k}}\left(x^{p_1^{r_1-1}}\right) = \cdots = \Phi_{p_1 p_2 \cdots p_k}\left(x^{p_1^{r_1-1} p_2^{r_2-1} \cdots p_k^{r_k-1}}\right).$$

5pt **13.6.10.** *Let ϕ denote the Frobenius automorphism of $\mathbb{F}_{p^n}$, $\phi(\alpha) = \alpha^p$. Prove that the order of ϕ (as an element of the group of automorphisms of $\mathbb{F}_{p^n}$) is n.*

Solution. Since the multiplicative group $\mathbb{F}_{p^n}^*$ of $\mathbb{F}_{p^n}$ has order $p^n - 1$, every $\alpha \in \mathbb{F}_{p^n}^*$ satisfies $\alpha^{p^n-1} = 1$, so $\alpha^{p^n} = \alpha$. This is also true for $\alpha = 0$, so for every $\alpha \in \mathbb{F}_{p^n}$, $\phi^n(\alpha) = \alpha^{p^n} = \alpha$, and thus $\phi^n = \mathrm{Id}$.

On the other hand, for any $k < n$, the polynomial $x^{p^k} - x$ cannot have more than p^k roots in $\mathbb{F}_{p^n}$, so, not all elements $\alpha \in \mathbb{F}_{p^n}$ satisfy $\phi^k(\alpha) = \alpha$, so $\phi^k \neq \mathrm{Id}$.

5pt **14.3.4.** *Construct the field $\mathbb{F}_{16}$ and find a generator of its multiplicative group.*

Solution. To construct $\mathbb{F}_{16}$ we can use any irreducible quartic polynomial over $\mathbb{F}_2$; take $f = x^4 + x + 1$ and put $K = \mathbb{F}_2[x]/(f)$. Let α be the image of x in K, then $\alpha^4 = -\alpha - 1 = \alpha + 1$. Now, $\mathbb{F}_{16} \cong K = \left\{a + b\alpha + c\alpha^2 + d\alpha^3,\ a, b, c, d \in \mathbb{F}_2\right\}$ with $\alpha^4 = 1 + \alpha$.

The multiplictive group $\mathbb{F}_{16}^*$ is isomorphic to $\mathbb{Z}_{15}$ and has $\varphi(15) = 2 \cdot 4 = 8$ generators. Let us try α: we have $1, \alpha, \alpha^2, \alpha^3$ all distinct, then $\alpha^4 = 1 + \alpha$, $\alpha^5 = \alpha + \alpha^2$, $\ldots$, – we don't need to check the powers of α further since we already see that $|\alpha| > 5$, and hence $|\alpha| = 15$.

10pt **A4.** (a) *Find all irreducible polynomials of degree 4 in $\mathbb{F}_2[x]$.*

Solution. Let $\psi(n)$ denote the number of irreducible polynomials of degree n in $\mathbb{F}_2[x]$. Then, by the general formula, $\psi(1) = 2$; $1\psi(1) + 2\psi(2) = 4$ so $\psi(2) = 1$; $1\psi(1) + 3\psi(1) = 8$ so $\psi(3) = 2$; $1\psi(1) + 2\psi(2) + 4\psi(4) = 16$, so $\psi(4) = 3$.

An irreducible polynomial of degree ≥ 2 in $\mathbb{F}_2[x]$ must not vanish at 0 and 1, so it must end with 1 and have an odd number of monomials. Also, if all monomials of a polynomial f have even power, then f is a square (for example, $x^4 + 1 = (x^2 + 1)^2$ and $x^4 + x^2 + 1 = (x^2 + x + 1)^2$). So, the irreducible polynomials of degree 4 are $x^4 + x^3 + 1$, $x^4 + x + 1$, and $x^4 + x^3 + x^2 + x + 1$.

5pt (b) *Determine the number of monic irreducible polynomials of degree 4 in $\mathbb{F}_3[x]$.*

Solution. Let $\psi(n)$ denote the number of monic irreducible polynomials of degree n in $\mathbb{F}_3[x]$. Then $\psi(1) = 3$, $1\psi(1) + 2\psi(2) = 9$ so $\psi(2) = 3$, and $1\psi(1) + 2\psi(2) + 4\psi(4) = 81$, so $\psi(4) = 18$.