Answersheet 13 - Yiwei Yang 2018533218

1.

($\rightarrow$) First A field of characteristic 0 is perfect. Then let F be a field of characteristic $p \neq 0$. Suppose that a and b are elements of F. Then $(a+b)^p = a^p + b^p$. In particular, the function $\Phi_F : F \rightarrow F$ defined by $\Phi_F(x) = x^p$ is a homomorphism.

Proof. Expand $(a+b)^p$ using the binomial theorem. All of the binomial coefficients are divisible by p, except for the first and last ones.

($\leftarrow$) First, let F be field and let $f(x) \in F[x]$ be an irreducible polynomial. If $f(x)$ is not separable then $f'(x) = 0$.

Proof. Suppose that $f(x)$ is not separable and that $f'(x) \neq 0$. Since $f(x)$ is irreducible, and $f'(x)$ has lower degree than $f(x)$, the greatest common divisor of f and f' is 1 . Let $a(x)$ and $b(x)$ be polynomials in $F[x]$ such that $a(x)f(x) + b(x)f'(x) = 1$.

Since f is not separable, there is an extension K of F such that f has a repeated root $\alpha \in K$. Thus in $K[x]$ we have $f(x) = (x-\alpha)^2 h(x)$. By the product rule, $f'(x) = 2(x-\alpha)h(x) + (x-\alpha)^2 h'(x)$. Thus $f(\alpha) = f'(\alpha) = 0$
Since the equation $a(x)f(x) + b(x)f'(x) = 1$ holds in $F[x]$, it also holds in $K[x]$ when we regard a, b, f and f' as polynomials in $K[x]$. But this is absurd since $a(\alpha)f(\alpha) + b(\alpha)f'(\alpha) = 0$ in $K[x]$. This contradiction shows that $f'(x) = 0$.

Then let F be field and let $f(x) \in F[x]$ be a polynomial of positive degree. If $f'(x) = 0$ then Char $F = p$ for some prime p and $f(x) = g(x^{np})$ for some $n > 0$ and some polynomial $g(x)$ with $g'(x) \neq 0$. In particular, if f is monic and irreducible, but not separable, then $f(x) = g(x^{np})$ where $n > 0$ and g is monic, irreducible and separable.
Proof. Suppose that $f'(x) = 0$. Write $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Consider a monomial $a_k x^k$ where $a_k \neq 0$. Since $f'(x) = 0$ we have $k a_k x^k = 0$, so F must have non-zero characteristic p and k must be divisible by p. Thus the non-zero monomials in f all have degree divisible by p. Let np be the greatest common divisor of the degrees of the non-zero monomials that occur in f. We have $f(x) = g(x^{np})$, where the coefficients of g are the same as those of f, but of different degree. There is at least one non-zero monomial in g with degree not divisible by p. Thus $g'(x) \neq 0$. Any factorization of g yields a factorization of f by substituting x^{np} for x. Thus g is irreducible whenever f is irreducible.

Finally, if F is a field of characteristic $p \neq 0$ and if the Frobenius endomorphism $\Phi_F : F \rightarrow F$ is surjective, then F is perfect.

Proof. Let F be a perfect field and consider a monic irreducible polynomial $f(x) \in F[x]$ of degree m. Suppose that $f(x)$ is not separable. Then, according to first 2 part we must have Char $F = p \neq 0$ and we can write $f(x) = g(x^{np})$ for some separable polynomial g. A polynomial in x^{np} can also be regarded as a polynomial in x^p, so it implies that $f(x) = h(x)^p$ for some polynomial $h(x) \in F[x]$. This contradicts the irreducibility of f.

2.

a.

Assume that all fields are of characteristic p. Suppose that F/E_1 is separable, and E_1/E is separable. Let S be the set of all elements of F that are separable over E. Then $E_1 \subseteq S$, since E_1/E is separable.

Note that S is a subfield of F : indeed, if $u, v \in S$ and $v \neq 0$, then $E(u, v)$ is separable over E because it is generated by separable elements, so $u+v, u-v, uv$, and u/v are all separable over E. So S is a field.

I claim that F is purely inseparable over S. Indeed, if $u \in F$, then there exists $n \geq 0$ such that u^{p^n} is separable over E, hence there exists $n \geq 0$ such that $u^{p^n} \in S$. Therefore, the minimal polynomial of u over S is a divisor of $x^{p^n} - u^{p^n} = (x-u)^{p^n}$, so F is purely inseparable over S. But since $E_1 \subseteq S \subseteq F$, and F is separable over E_1, then it is separable over S. So F is both purely inseparable and separable over S. This can only occur if $S = F$, hence every element of S is separable over E.

b.

Given the equivalent of above. If the implication holds for all finite dimensional extensions, then we would have that $E_1(u_1, \ldots, u_n)$ is a Galois extension of E_1, and therefore there exist $\tau \in \operatorname{Aut}_{E_1}(E_1(u_1, \ldots, u_n))$ such that $\tau(u) \neq u$. Since E_2 is a splitting field over E_1, it is also a splitting field over $E_1(u_1, \ldots, u_n)$, and therefore τ extends to an automorphism of E_2. Thus, there exists $\tau \in \operatorname{Aut}_{E_1}(E_2)$ such that $\tau(u) \neq u$. This would prove that the fixed field of $\operatorname{Aut}_{E_1}(E_2)$ is E_1, so the extension is Galois. Thus, we are reduced to proving the implication when $[E_2 : E_1]$ is finite. When $[E_2 : E_1]$ is finite, there is a finite subset of T that will suffice to generate E_2. Moreover, $\operatorname{Aut}_{E_1}(E_2)$ is finite. If E is the fixed field of $\operatorname{Aut}_{E_1}(E_2)$, then by Artin's Theorem E_2 is Galois over E and $\operatorname{Gal}(E_2/E) = \operatorname{Aut}_{E_1}(E_2)$. Hence, $[E_2 : E] = |\operatorname{Aut}_{E_1}(E_2)|$
Thus, it suffices to show that when E_2 is a finite extension of E_1 and is a splitting field of a finite set of separable polynomials $g_1, \ldots, g_m \in E_1[x]$, then $[E_2 : E_1] = |\operatorname{Aut}_{E_1}(E_2)|$. Replacing the set with the set of all irreducible factors of the g_i, we may assume that all g_i are irreducible.

We do induction on $[E_2 : E_1] = n$. If $n = 1$, then the equality is immediate. If $n > 1$, then some g_i, say g_1, has degree greater than 1 ; let $u \in E_2$ be a root of g_1. Then $[E_1(u) : E_1] = \deg(g_1)$, and the number of distinct roots of g_1 in E_2 is $\deg(g_1)$, since g_1 is separable. Let $H = \operatorname{Aut}_{E_1(u)}(E_2)$. Define a map from the set of left cosets of H in $\operatorname{Aut}_{E_1}(E_2)$ to the set of distinct roots of g_1 in E_2 by mapping σH to $\sigma(u)$. This is one-to-one, since $\sigma(u) = \rho(u) \Longrightarrow \sigma^{-1}\rho \in H \Longrightarrow \sigma H = \rho H$. Therefore, $[\operatorname{Aut}_{E_1}(E_2) : H] \leq \deg(g_1)$. If $v \in E_2$ is any other root of g_1, then there is an isomorphism $\tau : E_1(u) \rightarrow E_1(v)$ that fixes E_1 and maps u to v, and since E_2 is a splitting field, τ extends to an automorphism of E_2 over E_1. Therefore, the map from cosets of H to roots of g_1 is onto, so $[\operatorname{Aut}_{E_1}(E_2) : H] = \deg(g_1)$
We now apply induction: E_2 is the splitting field over $E_1(u)$ of a set of separable polynomials (same one as we started with), and $[E_2 : E_1(u)] = [E_2 : E_1]/\deg(g_1) < [E_2 : E_1]$. Therefore, $[E_2 : E_1(u)] = |\operatorname{Aut}_{E_1(u)}(E_2)| = |H|$
Hence
$|\operatorname{Aut}_{E_1}(E_2)| = [\operatorname{Aut}_{E_1}(E_2) : H]\,|H| = \deg(g_1)[E_2 : E_1(u)] = [E_1(u) : E_1][E_2 : E_1(u)] = [E_2 : E_1]$
, and we are done.

3.

Proof. Choose a basis S for E_1 over E, and consider the subset E of F consisting of linear combinations of the elements of S with coefficients in E_2 :

$$E=\left\{\sum_{s\in S}\lambda_s s \mid \lambda_s\in E_2\right\}$$

Since 1 is in $\bar{E}_1$ and S spans $\bar{E}_1$ over E, there are elements ϵ_s of E such that

$$1=\sum_{s\in S}\epsilon_s s$$

Hence for any x in E_2,

$$x=\sum_{s\in S}\left(x\epsilon_s\right)s$$

is an element of E. Since E_1 is closed under multiplication, for every t and u in S there are elements $\mu_s^{t,u}$ of E such that

$$tu=\sum_{s\in S}\mu_s^{t,u}s$$

Hence for elements $x=\sum_{s\in S}\lambda_s s$ and $y=\sum_{s\in S}\nu_s s$ of E,

$$x+y=\sum_{s\in S}\left(\lambda_s+\nu_s\right)s$$

is in E and

$$\begin{aligned} xy=\sum_{t\in S,u\in S}\lambda_t\nu_u tu &= \sum_{t\in S,u\in S}\lambda_t\nu_u\left(\sum_{s\in S}\mu_s^{t,u}s\right)\\ &=\sum_{s\in S}\left(\sum_{t\in S,u\in S}\lambda_t\nu_u\mu_s^{t,u}\right)s\end{aligned}$$

is an element of E. So E contains E_2 and is closed under addition and multiplication. Eurthermore, S spans E as a vector space over E_2, so E is finitedimensional over E_2, of dimension at most $|S|=[E_1:E]$. Hence by Lemma 2.4, E is a subfield of F. Since E contains both E_1 and E_2, and is generated by elements of E_1E_2, $E=E_1E_2$. By the Tower Law, E_1E_2/E is finite, and $[E_1E_2:E]=[E_1E_2:E_2][E_2:E]\leq[E_1:E][E_2:E]$ as required

4.

The largest Field is $\mathrm{F}\left(X^{\frac{1}{2p}}\right)$.

Proof. Let ζ be the primitive n -th root in F. We have $(-\zeta)^{2n}=1$. Note that $\zeta\neq-\zeta$ because $\operatorname{char}(F)\neq 2$. Let us denote $-\zeta$ by ω and we claim that ω is the required primitive $2n$ -th root of unity. If not, let ω be a primitive d -th root of unity for $d<2n$. Hence

$$\omega^d=1\Rightarrow\zeta^d=(-1)^d.$$

Now there are two possibilities. If d is odd, then

$$\zeta^d=-1\Rightarrow\zeta^{2d}=1\Rightarrow n\mid 2d$$

(by definition of ζ). As n is odd, we must have $n\mid d$. Hence the only possibility is $d=n$, but clearly $\omega^n\neq 1$. So we arrive at a contradiction. If d is even, then

$$\zeta^d=1\Rightarrow n\mid d$$

Following the same argument as before we again arrive at a contradiction. Hence ω is the required $2n$ -th root of unity contained in F.