Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

December 5, 2020

Problems in Section 5.5.

1. If F is of characteristic 0 and $f(x) \in F[x]$ in such that $f'(x) = 0$, prove that $f(x) = \alpha \in F$.

Proof. Note that in the field F of characteristic 0, for any $a \in F$, $na = 0$ if and only if $n = 0$ or $a = 0$. Suppose we have $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$. If $f'(x) = 0$, we have $ka_k = 0$ for all $k = 1, 2, \cdots, n$. This forces that $a_k = 0$ for all $k = 1, 2, \cdots, n$ and hence, $f(x) = a_0$ for some $a_0 \in F$. □

2. If F is of characteristic $p \neq 0$ and if $f(x) \in F[x]$ is such that $f'(x) = 0$, prove that $f(x) = g(x^p)$ for some polynomial $g(x) \in F[x]$.

Proof. Note that in the field F of characteristic 0, for any $a \in F$, $na = 0$ if and only if $p \mid n$ or $a = 0$. Suppose we have $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$. If $f'(x) = 0$, we have $ka_k = 0$ for all $k = 1, 2, \cdots, n$ which implies that coefficients of x^t, where t is not a divisor of prime, vanish. Ultimately, we have $f(x)$ of the form $f(x) = a_{pk_m} x^{pk_m} + a_{pk_{m-1}} x^{pk_{m-1}} + \cdots + a_p x^p + a_0$. □

3. Prove that $(f(x)+g(x))' = f'(x)+g'(x)$ and that $(\alpha f(x))' = \alpha f'(x)$ for $f(x), g(x) \in F[x]$ and $\alpha \in F$.

Proof. Let $f(x) = \sum_i^n a_i x^i$, $g(x) = \sum_i^m b_i x^i \in F[x]$. Let $c_i = a_i + b_i$. Denote $f(x) + g(x)$

by $\sum_i^t c_i x^i$. Consequently, we have

$$\begin{aligned}(f(x)+g(x))' &= \left(\sum_{i=0}^{t} c_i x^i\right)' = \sum_{i=0}^{t-1} i c_i x^{i-1} \\ &= \sum_{i=0}^{t-1} i(a_i+b_i)x^{i-1} \\ &= \sum_{i=0}^{t-1} i a_i x^{i-1} + \sum_{i=0}^{t-1} i b_i x^{i-1} \\ &= f'(x)+g'(x).\end{aligned}$$

Moreover,

$$\begin{aligned}(\alpha f(x))' &= \left(\alpha \sum_{i=0}^{n} a_i x^i\right)' = \left(\sum_{i=0}^{n} \alpha a_i x^i\right)' \\ &= \sum_{i=0}^{n-1} \alpha i a_i x^{i-1} = \alpha \sum_{i=0}^{n-1} i a_i x^{i-1} \\ &= \alpha f'(x).\end{aligned}$$

□

4. Prove that there is no rational function in $F(x)$ such that its square is x.

Proof. Let $r(x) = \dfrac{f(x)}{g(x)}$ denote a rational function in $F(x)$ where $f(x)$ and $g(x)$ are in $F[x]$. Suppose $r(x)^2 = x$. Then $f(x)^2 = xg(x)^2$. Note that the degree of $f(x)$ and $g(x)$ must be same. Let $\deg f(x) = k$. But we have that

$$\deg f(x)^2 = k^2 = \deg(xg(x)^2) = \deg x + \deg g(x)^2 = 1 + k^2,$$

which is a contradiction. Thus, there is no rational function in $F(x)$ such that its square is x. □

5. Complete the induction needed to establish the corollary to Theorem 5.5.1.

Proof. We have to show that, if $a_1, a_2, \cdots, a_n$ are algebraic over F, then there is $c \in F(a_1, a_2, \cdots, a_n)$ such that $F(c) = F(a_1, a_2, \cdots, a_n)$. If $n = 1$, it is trivial. So we assume that the statement is true for all $k < n$. Consider an extension field $F(a_1, a_2, \cdots, a_n)$. Then there is a $c' \in F(a_1, a_2, \cdots, a_{n-1})$ such that $F(c') = F(a_1, a_2, \cdots, a_{n-1})$. Hence, $F(a_1, a_2, \cdots, a_n) = (F(c'), a_n) = F(c', a_n)$. Applying the induction hypothesis again, we can find $c \in F(c', a_n)$ such that $F(c) = F(c', a_n) = F(a_1, a_2, \cdots, a_n)$. □

6. Show that any field of characteristic 0 is perfect.

Proof. Let E be a finite extension of field F(of characteristic 0) with degree n. Choose $\alpha \in E$. Consider the set $\{1, \alpha, \alpha^2, \cdots, \alpha^n\}$ in E. As $[E : F] = n$, the above set is linearly dependent over F and hence α admits a minimal polynomial $p(x)$ such that $p(\alpha) = 0$. But since every irreducible polynomial in the field of characteristic 0 has no multiple roots, it is separable. As α and E were arbitrary, F is perfect. □

7. a) If F is of characteristic $p \neq 0$ show that for $a, b \in F$, $(a+b)^{p^m} = a^{p^m} + b^{p^m}$.

Proof. Observe the following:

$$\begin{aligned}(a+b)^{p^m} &= \sum_{k=0}^{p^m} \binom{p^m}{k} a^{p^m-k} b^k \\ &= a^{p^m} + \binom{p^m}{1} a^{p^m-1} b + \binom{p^m}{2} a^{p^m-2} b^2 + \cdots + \binom{p^m}{p^m-1} a b^{p^m-1} + b^{p^m} \\ &= a^{p^m} + b^{p^m} \quad (\because p \mid \binom{p^m}{k},\ k \in \mathbb{Z}^+).\end{aligned}$$

□

b) If F is of characteristic $p \neq 0$ and if K is an extension of F let $T = \{a \in K : a^{p^n} \in F \text{ for some } n\}$. Prove that T is a subfield of K.

Proof. Suppose $a, b \in T$. Let n, m be the integers such that $a^{p^n}, b^{p^m} \in F$. Consequently,

$$(a+b)^{p^{n+m}} = a^{p^{n+m}} + b^{p^{n+m}} = (a^{p^n})^{p^m} + (b^{p^m})^{p^n} \in F.$$

Also,

$$(ab)^{p^{n+m}} = (a^{p^n})^{p^m} \cdot (b^{p^m})^{p^n} \in F.$$

Moreover,

$$1 = 1^{p^n} = \left(a \cdot \frac{1}{a}\right)^{p^n} = a^{p^n} \left(\frac{1}{a}\right)^{p^n} \implies \left(\frac{1}{a}\right)^{p^n} \in F.$$

Therefore, T forms a subfield of K. □

8. If K, T, F are as in Problem 7b) show that any automorphism of K leaving every element of F fixed also leaves every element of T fixed.

Proof. Let $\sigma \in \mathcal{A}(K)$ which fixes F. Choose $t \in T$. Then there is an integer n such that $t^{p^n} \in F$. Consequently, $\sigma(t)^{p^n} = \sigma(t^{p^n}) = t^{p^n}$. Recall that $charF = p$ so that $(\sigma(t) - t)^{p^n} = 0$. So the only possibility is that $\sigma(t) = t$. Hence, σ also fixes T. □

9. Show that a field F of characteristic $p \neq 0$ is perfect if and only if for every $a \in F$ we can find a $b \in F$ such that $b^p = a$.

Proof. Given statement is equivalent to that of: Every irreducible polynomial in $F[x]$ is separable if and only if $F^p = F$. We prove its contrapositive, that is there is an irreducible inseparable polynomial in $F[x]$ if and only if $F^p \neq F$.
Suppose $F^p \neq F$. Choose $a \in F - F^p$. Consider the polynomial $p(x) = x^p - a \in F[x]$. Suppose β is a root of $p(x)$ in the splitting field of $p(x)$ over F. Then

$$x^p - a = x^p - \beta^p = (x - \beta)^p$$

so that β is the only root of $p(x)$. We now claim that $p(x)$ is the polynomial we seek; an irreducible inseparable polynomial in $F[x]$. Note that any proper monic divising factor of $p(x)$(in the polynomial ring of the splitting field) is of the form $(x - \beta)^m$. Suppose it has to be a polynomial in $F[x]$, as the coefficient of x^{m-1} is $-m\beta$, $m\beta \in F$. Hence, $\beta \in F$. But this implies $\beta^p = a$, contradicting that $a \in F - F^p$. Therefore, $p(x)$ is an irreducible insparable polynomial in $F[x]$.
Conversely, assume that there is an irreducible inseparable polynomial $p(x)$ in $F[x]$. Then $p(x) = g(x^p)$ for some $g(x) \in F[x]$. If $F^p = F$, for each $a \in F$, there is $b \in F$ such that $b^p = a$. Writing $p(x) = g(x^p) = a_{pk_m}x^{pk_m} + a_{pk_{m-1}}x^{pk_{m-1}} + \cdots + a_p x^p + a_0$, we have

$$\begin{aligned} p(x) &= (b_m x^{k_m})^p + (b_{m-1}x^{k_{m-1}})^p + \cdots + (b_1 x)^p + b_0^p, \quad (b_m^p = a_{pk_m}) \\ &= (b_m x^{k_m} + b_{m-1}x^{k-m-1} + \cdots + b_1 x + b_0)^p \end{aligned}$$

so that $p(x)$ is reducible. But this contradicts the irreducibility of $p(x)$. Hence, $F^p \neq F$. □

10. Using the result of Problem 9, prove that any finite field is perfect.

Proof. Consider the Frobenius mapping $\sigma : F \to F$ sending $x \mapsto x^p$. It is clearly an injective homomorphism. Since F is given finite, σ is also surjective. Therefore, $F^p = F$, and hence, by Problem 9 the given finite field F is perfect. □

11. If K is an extension of F prove that the set of elements in K which are separable over F forms a subfield of K.

Proof. I could not yet find a proof that does not make use of notion of separable degree. I shall give a note on separable degree or find a proof that can be considered more elementary; a proof does not involve any other than introduced in the text of Herstein's. □

12. If F is of characteristic $p \neq 0$ and if K is a finite extension of F, prove that given $a \in K$ either $a^{p^n} \in F$ for some n or we can find an integer m such that $a^{p^m} \notin F$ and is separable over F.

Proof. If $\alpha \in K$ is separable over F, then there is nothing to prove. So we assume that α is inseparable over F. That is, for any irreducible polynomial $f(x) \in F[x]$ that α satisfies, $f(x) = g(x^p)$ for some $g(x) \in F[x]$. Choose the maximal integer m such that $f(x) = h(x^{p^m})$ for some $h(x) \in F[x]$. Now the obtained $h(x)$ is a polynomial that is both irreducible and not a polynomial of the form of $t(x^p), t(x) \in F[x]$, by the definition of m. Hence, $h(x)$ is separable over F. If $\alpha^{p^m} \in F$, we are done. If not, then α^{p^m} is a root of $h(x)$, which does not lie in F and separable over F. □

13. If K and F are as in Problem 12, and if no elements which is in K but not in F is separable over F, prove that given $a \in K$ we can find an integer n, depending on a, such that $a^{p^n} \in F$.

Proof. If $\alpha \in F$, we are done. If $\alpha \in K - F$, α must satisfy either $a^{p^n} \in F$ for some n or $a^{p^m} \notin F$ and a^{p^m} is separable over F. But clearly, later is not the case as no elements in $K - F$ is separable. Hence, $a^{p^n} \in F$ for some n(depending on a). □

14. If K is a finite, separable extension of F prove that K is a simple extension of F.

Proof. If F has characteristic 0, then it is just the same as Theorem 5.5.1. So we handle the case of F having characteristic $p \neq 0$. We have two cases: i) F is a finite field and ii) F is infinite.
If F is a finite field, so does K and hence, $K^\times$, is a cyclic group under multiplication(Problem 9, Section 5.1). Hence, it admits generator α(in K) and hence, $K = F(\alpha)$.
If F is infinite, we just follow the method used for the proof of Theorem 5.5.1. First consider the finite extension $F(\alpha, \beta)$ of F to be separable. Let $f(x)$ and $g(x)$ be the irreducible polynomials of degree m and n, satisfied by α and β respectively. As α and β were separable, $f(x)$ and $g(x)$ could chosen to be separable over F. That is, every roots of $f(x)$ are distinct and so does $g(x)$. Let the roots of $f(x)$ be $a = a_1, a_2, \cdots, a_m$ and the roots of $g(x)$ be $b = b_1, b_2, \cdots, b_n$. Since F is infinite, we could have chose $\gamma \in F$ such that $a_i + \gamma b_j \neq a + \gamma b$ for all i and j. Put $c = a + \gamma b$. Then $F(c) \subset F(a, b)$.
Now, as b satisfies $g(x) \in F[x]$, $g(x)$ can be considered as a polynomial over $F(c)$. Moreover, if $h(x) = f(c - \gamma x)$ then $h(x) \in F(c)$ and $h(b) = f(c - \gamma b) = f(a) = 0$, so that $(x - b) \mid g(x), h(x)$ in some extension of $F(c)$. Suppose b_j was another root of $g(x)$, then $h(b_j) = f(c - \gamma b_j) \neq 0$ unless $b_j = b$. Also, as $g(x)$ is separable, it has no multiple root. Hence, $x - b$ is the greatest common divisor of $h(x)$ and $g(x)$ over some extension of $F(c)$. Note that $\deg x - b = 1$. Hence, the nontrivial greatest common divisor of $h(x)$ and $g(x)$ in $F(c)[x]$, which must be a divisor of $x - b$, is exactly $x - b$ itself. Hence, $b \in F(c)$. As $a = c - \gamma b \in F(c)$, $a, b \in F(c)$ and hence, $F(a, b) \subset F(c)$. Therefore, combining the result, we have $F(a, b) = F(c)$ given that $F(a, b)$ is separable(or equivalently, a, b are separable) over F.
So now by induction, we have that finite separable extension K of F is a simple extension of F. □

15. If one of a or b is separable over F, prove that $F(a, b)$ is a simple extension of F.

Proof. Scrutinising the proof of Problem 14 or Theorem 5.5.1, we can see that choosing of value $\gamma \in F$ for the primitive c, depends on the choosing of roots of $f(x)$ and $g(x)$. In general, although $f(x)$ is not be separable, we still can choose c so that $c = a+\gamma b \neq a_i+\gamma b_j$ for all i and j. The place where the separability of b used is to show the existence of monic greatest common divisor of $h(x)$ and $g(x)$. Thus, separability of only either one of a or b is sufficient to prove that $F(a, b)$ is a simple extension of F. □