

(March 14, 2005)

Solutions 15

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/~garrett/

[15.1] Let k be a field of characteristic 0. Let f be an irreducible polynomial in $k[x]$. Prove that f has no repeated factors, even over an algebraic closure of k .

If f has a factor P^2 where P is irreducible in $k[x]$, then P divides $\gcd(f, f') \in k[x]$. Since f was monic, and since the characteristic is 0, the derivative of the highest-degree term is of the form nx^{n-1} , and the coefficient is non-zero. Since f' is not 0, the degree of $\gcd(f, f')$ is at most $\deg f'$, which is strictly less than $\deg f$. Since f is irreducible, this \gcd in $k[x]$ must be 1. Thus, there are polynomials a, b such that $af + bf' = 1$. The latter identity certainly persists in $K[x]$ for any field extension K of k . ///

[15.2] Let K be a finite extension of a field k of characteristic 0. Prove that K is separable over k .

Since K is finite over k , there is a finite list of elements $\alpha_1, \dots, \alpha_n$ in K such that $K = k(\alpha_1, \dots, \alpha_n)$. From the previous example, the minimal polynomial f of α_1 over k has no repeated roots in an algebraic closure \bar{k} of k , so $k(\alpha_1)$ is separable over k .

We recall^[1] the fact that we can map $k(\alpha_1) \rightarrow \bar{k}$ by sending α_1 to any of the $[k(\alpha_1) : k] = \deg f$ distinct roots of $f(x) = 0$ in \bar{k} . Thus, there are $[k(\alpha_1) : k] = \deg f$ distinct distinct imbeddings of $k(\alpha_1)$ into \bar{k} , so $k(\alpha_1)$ is separable over k .

Next, observe that for any imbedding $\sigma : k(\alpha_1) \rightarrow \bar{k}$ of $k(\alpha_1)$ into an algebraic closure \bar{k} of k , by proven properties of \bar{k} we know that \bar{k} is an algebraic closure of $\sigma(k(\alpha_1))$. Further, if $g(x) \in k(\alpha_1)[x]$ is the minimal polynomial of α_2 over $k(\alpha_1)$, then $\sigma(g)(x)$ (applying σ to the coefficients) is the minimal polynomial of α_2 over $\sigma(k(\alpha_1))$. Thus, by the same argument as in the previous paragraph we have $[k(\alpha_1, \alpha_2) : k(\alpha_1)]$ distinct imbeddings of $k(\alpha_1, \alpha_2)$ into \bar{k} for a given imbedding of $k(\alpha_1)$. Then use induction. ///

[15.3] Let k be a field of characteristic $p > 0$. Suppose that k is **perfect**, meaning that for any $a \in k$ there exists $b \in k$ such that $b^p = a$. Let $f(x) = \sum_i c_i x^i$ in $k[x]$ be a polynomial such that its (algebraic) derivative

$$f'(x) = \sum_i c_i i x^{i-1}$$

is the zero polynomial. Show that there is a unique polynomial $g \in k[x]$ such that $f(x) = g(x)^p$.

For the derivative to be the 0 polynomial it must be that the characteristic p divides the exponent of every term (with non-zero coefficient). That is, we can rewrite

$$f(x) = \sum_i c_{ip} x^{ip}$$

Let $b_i \in k$ such that $b_i^p = c_{ip}$, using the perfect-ness. Since p divides all the inner binomial coefficients $p^i / i!(p-i)!$,

$$\left(\sum_i b_i x^i \right)^p = \sum_i c_{ip} x^{ip}$$

as desired. ///

[15.4] Let k be a perfect field of characteristic $p > 0$, and f an irreducible polynomial in $k[x]$. Show that f has no repeated factors (even over an algebraic closure of k).

[1] Recall the proof: Let β be a root of $f(x) = 0$ in \bar{k} . Let $\varphi : k[x] \rightarrow k[\beta]$ by $x \rightarrow \beta$. The kernel of φ is the principal ideal generated by $f(x)$ in $k[x]$. Thus, the map φ factors through $k[x]/\langle f \rangle \approx k[\alpha_1]$.

If f has a factor P^2 where P is irreducible in $k[x]$, then P divides $\gcd(f, f') \in k[x]$. If $\deg \gcd(f, f') < \deg f$ then the irreducibility of f in $k[x]$ implies that the \gcd is 1, so no such P exists. If $\deg \gcd(f, f') = \deg f$, then $f' = 0$, and (from above) there is a polynomial $g(x) \in k[x]$ such that $f(x) = g(x)^p$, contradicting the irreducibility in $k[x]$. ///

[15.5] Show that all finite fields \mathbf{F}_{p^n} with p prime and $1 \leq n \in \mathbf{Z}$ are perfect.

Again because the inner binomial coefficients $p!/i!(p-i)!$ are 0 in characteristic p , the (Frobenius) map $\alpha \rightarrow \alpha^p$ is not only (obviously) multiplicative, but also additive, so is a ring homomorphism of \mathbf{F}_{p^n} to itself. Since $\mathbf{F}_{p^n}^\times$ is cyclic (of order p^n), for any $\alpha \in \mathbf{F}_{p^n}$ (including 0)

$$\alpha^{(p^n)} = \alpha$$

Thus, since the map $\alpha \rightarrow \alpha^p$ has the (two-sided) inverse $\alpha \rightarrow \alpha^{p^{n-1}}$, it is a bijection. That is, everything has a p^{th} root. ///

[15.6] Let K be a finite extension of a finite field k . Prove that K is separable over k .

That is, we want to prove that the number of distinct imbeddings σ of K into a fixed algebraic closure \bar{k} is $[K : k]$. Let $\alpha \in K$ be a generator for the cyclic group K^\times . Then $K = k(\alpha) = k[\alpha]$, since powers of α already give every element but 0 in K . Thus, from basic field theory, the degree of the minimal polynomial $f(x)$ of α over k is $[K : k]$. The previous example shows that k is perfect, and the example before that showed that irreducible polynomials over a perfect field have no repeated factors. Thus, $f(x)$ has no repeated factors in any field extension of k .

We have also already seen that for algebraic α over k , we can map $k(\alpha)$ to \bar{k} to send α to *any* root β of $f(x) = 0$ in \bar{k} . Since $f(x)$ has not repeated factors, there are $[K : k]$ distinct roots β , so $[K : k]$ distinct imbeddings. ///

[15.7] Find all fields intermediate between \mathbf{Q} and $\mathbf{Q}(\zeta)$ where ζ is a primitive 17^{th} root of unity.

Since 17 is prime, $\text{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \approx (\mathbf{Z}/17)^\times$ is cyclic (of order 16), and we know that a cyclic group has a unique subgroup of each order dividing the order of the whole. Thus, there are intermediate fields corresponding to the proper divisors 2, 4, 8 of 16. Let σ_a be the automorphism $\sigma_a \zeta = \zeta^a$.

By a little trial and error, 3 is a generator for the cyclic group $(\mathbf{Z}/17)^\times$, so σ_3 is a generator for the automorphism group. Thus, one reasonably considers

$$\begin{aligned} \alpha_8 &= \zeta + \zeta^{3^2} + \zeta^{3^4} + \zeta^{3^6} + \zeta^{3^8} + \zeta^{3^{10}} + \zeta^{3^{12}} + \zeta^{3^{14}} \\ \alpha_4 &= \zeta + \zeta^{3^4} + \zeta^{3^8} + \zeta^{3^{12}} \\ \alpha_2 &= \zeta + \zeta^{3^8} = \zeta + \zeta^{-1} \end{aligned}$$

The α_n is visibly invariant under the subgroup of $(\mathbf{Z}/17)^\times$ of order n . The linear independence of $\zeta, \zeta^2, \zeta^3, \dots, \zeta^{16}$ shows α_n is *not* by accident invariant under any larger subgroup of the Galois group. Thus, $\mathbf{Q}(\alpha_n)$ is (by Galois theory) the unique intermediate field of degree $16/n$ over \mathbf{Q} .

We can also give other characterizations of some of these intermediate fields. First, we have already seen (in discussion of Gauss sums) that

$$\sum_{a \bmod 17} \left(\frac{a}{17}\right)_2 \cdot \zeta^a = \sqrt{17}$$

where $\left(\frac{a}{17}\right)_2$ is the quadratic symbol. Thus,

$$\begin{aligned} \alpha_8 - \sigma_3 \alpha_8 &= \sqrt{17} \\ \alpha_8 + \sigma_3 \alpha_8 &= 0 \end{aligned}$$

so α_8 and $\sigma_3 \alpha_8$ are $\pm\sqrt{17}/2$. Further computation can likewise express all the intermediate fields as being obtained by adjoining square roots to the next smaller one. ///

[15.8] Let f, g be *relatively prime* polynomials in n indeterminates t_1, \dots, t_n , with g not 0. Suppose that the ratio $f(t_1, \dots, t_n)/g(t_1, \dots, t_n)$ is invariant under all permutations of the t_i . Show that both f and g are polynomials in the elementary symmetric functions in the t_i .

Let s_i be the i^{th} elementary symmetric function in the t_j 's. In the previous batch of examples we showed that $k(t_1, \dots, t_n)$ has Galois group S_n (the symmetric group on n letters) over $k(s_1, \dots, s_n)$. Thus, the given ratio lies in $k(s_1, \dots, s_n)$. Thus, it is *expressible* as a ratio

$$\frac{f(t_1, \dots, t_n)}{g(t_1, \dots, t_n)} = \frac{F(s_1, \dots, s_n)}{G(s_1, \dots, s_n)}$$

of polynomials F, G in the s_i . Perhaps it is wisest to stop here for the moment, delaying the discussion of the invariance of the original f, g themselves. ///