Graded

1. (13.5.5) For any prime p and any nonzero $a \in \mathbb{F}_p$ prove that $x^p - x + a$ is irreducible and separable over $\mathbb{F}_p$. [For the irreducibility: One approach — prove first that if α is a root then $\alpha + 1$ is also a root. Another approach — suppose it's reducible and compute derivatives.]

   Proof. Let $f(x) = x^p - x + a \in \mathbb{F}_p$ as above. To see separability of $f(x)$, observe that the derivative $D_x(f(x))$ is $px^{p-1} - 1 = -1$ so that $\gcd(f(x), D_x(f(x))) = 1$, implying $f(x)$ is separable. (We could also have shown that $f(x)$ was irreducible over $\mathbb{F}_p$, a finite field as below.)

   We prove that $f(x)$ is irreducible. Let α be a root of $f(x)$. Then for any $t \in \mathbb{F}_p$ we use the Frobenius endomorphism and Fermat's little theorem (or one could argue with binomial coefficients) to see that

   $$f(\alpha + t) = (\alpha + t)^p - (\alpha + t) + a = (\alpha^p - \alpha + a) + t^p - t = 0.$$

   It follows that $\alpha + t$ is a root of $f(x)$ for each $t \in \mathbb{F}_p$. Note that there are no roots of $f(x)$ lying in $\mathbb{F}_p$ since by Fermat's little theorem $b^p - b = 0$ for any $b \in \mathbb{F}_p$.

   Let $m_\alpha(x)$ be the minimal polynomial for α over $\mathbb{F}_p$. For each t, $m_\alpha(x - t)$ is also monic and irreducible and has $\alpha + t$ as a root, so it must be the minimal polynomial for $\alpha + t$. The degree of each of these minimal polynomials $m_\alpha(x - t)$ for each t are the same, and moreover cannot be 1 since $\alpha + t$ is not found in $\mathbb{F}_p$. For any $t_1, t_2 \in \mathbb{F}_p$ with $t_1 \neq t_2$, roots of $m_\alpha(x - t_1)$ and $m_\alpha(x - t_1)$ are disjoint since otherwise the two polynomials would have to divide each other as they are minimal polynomials, but this would mean they were the same polynomial – impossible.

   We know that the degrees of these minimal polynomials is at least 2, but we want to show that they are each of degree p so that they are actually all the same polynomial, $f(x)$ (since $f(x)$ is a degree p polynomial and each minimal polynomial divides $f(x)$).

   Suppose not, so that the degree of $m_\alpha(x - t)$ for each t is some j for $2 \leq j \leq p - 1$. Since each of the $\alpha + t$ are roots of $f(x)$, we have that there is a subset $A \subset \{m_\alpha(x - t) \mid t \in \mathbb{F}_p\}$ for which the product $\prod_{m(x) \in A} m(x)$ divides $f(x)$ and every $\alpha - t$ is a root of the product. But the degree of the product is $j \cdot |A|$, which is equal to p, a prime. So one of j or $|A|$ has to be 1, but $|A|$ cannot be p since we saw that $m_\alpha(x - t)$ for any t is not linear. So j must be p, from which it follows that $m_\alpha(x)$ is $f(x)$, meaning $x^p - x + a$ is irreducible. □

2. (Problem 1) Let K be the splitting field of $x^4 - 2$ over $\mathbb{Q}$. Carefully determine $[K : \mathbb{Q}]$, and use this to show that $x^4 - 2$ is irreducible over $\mathbb{Q}(i)$. (Suggestion: pay attention to which fields are subfields of $\mathbb{R}$.)

   Proof. Factoring over $\mathbb{C}$ to identify roots, we find that the four roots of $f(x) = x^4 - 2$ are $\pm 2^{1/4}$ and $\pm i 2^{1/4}$. We show that $K = \mathbb{Q}(2^{1/4}, i)$ is the splitting field for $f(x)$ over $\mathbb{Q}$, and that $[K : \mathbb{Q}] = 8$.

   The field K is a field that contains all four roots of $f(x)$, so the splitting field for $f(x)$ is contained in K. The reverse inclusion may be found by seeing that no smaller subfield of K allows $f(x)$ to split (we have $\mathbb{Q}(2^{1/4}) \subset \mathbb{R}$ and $\mathbb{Q}(i) \subset \mathbb{C}$ and not adjoining either of $2^{1/4}$ or i will not permit $f(x)$ to split).

Observe that $\mathbb{Q}(2^{1/4})$ is a degree 4 extension of $\mathbb{Q}$ since x^4-2 is the minimal polynomial for $2^{1/4}$ (it is monic and Eisenstein at $p=2$). Then by adjoining i to $\mathbb{Q}(2^{1/4})$ we obtain K; and this is a degree 2 extension since the monic polynomial x^2+1 has no roots in $\mathbb{Q}(2^{1/4})$ (the roots $\pm i$ are in $\mathbb{C}$ but $\mathbb{Q}(2^{1/4}) \subset \mathbb{R}$). By multiplicativity of field extension degrees we have $[K\colon \mathbb{Q}] = 8$.

Similarly, we can start by adjoining i to $\mathbb{Q}$ (a degree 2 extension) and since $[K\colon \mathbb{Q}] = 8$, it follows that adjoining $2^{1/4}$ to $\mathbb{Q}(i)$ must be a degree 4 extension. So the minimal polynomial of $2^{1/4}$ is monic and irreducible of degree 4 and must divide x^4-2; this is only possible if x^4-2 is the minimal polynomial of $2^{1/4}$ over $\mathbb{Q}(i)$. Hence x^4-2 is irreducible over $\mathbb{Q}(i)$. □

Additional Problems

1. (13.4.5) Let K be a finite extension of F. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$. [Use Theorems 8 and 27.]

   Proof. Let K be a finite extension of F as above. Suppose first that K is a splitting field over F for some polynomial $g(x) \in F[x]$. Then let $f(x) \in F[x]$ be irreducible with a root $\alpha \in K$. Then let α' be any other root of $f(x)$ (note that $\alpha, \alpha' \notin F$ since otherwise $f(x)$ would not be irreducible).

   Extend the identity map on F to an isomorphism ϕ of the field extensions $F(\alpha)$ and $f(\alpha')$ which is the identity map on elements of $F \subset F(\alpha)$.

   Observe that K is a splitting field of $F(\alpha)$ since $\alpha \in K$ and that the corresponding splitting field for $F(\alpha')$ is $K(\alpha')$ since it is the smallest field containing $F(\alpha')$ for which $g(x)$ viewed as an element of $F(\alpha')[x]$ splits completely.

   Thus we can extend ϕ into an isomorphism σ of K with $K(\alpha')$, so that $[K(\alpha')\colon F] = [K\colon F]$. But $[K(\alpha')\colon F] = [K(\alpha')\colon K][K\colon F]$, so by cancellation we have that $[K(\alpha')\colon K] = 1$, meaning that $\alpha' \in K$.

   Since α' was an arbitrary root of $f(x)$, it follows that $f(x)$ splits completely as desired.

   Conversely, write K as $F(\alpha_1, \ldots, \alpha_n)$ and suppose that every irreducible polynomial with a root in K splits completely. Consider the minimal polynomials $m_{\alpha_i}(x) \in F[x]$ for each α_i. We show that K is the splitting field for $f(x) = \prod_{i=1}^{n} m_{\alpha_i}(x)$ over F. It is true that each of the minimal polynomials has a root in K, so each splits completely; as a result $f(x)$ does in K also. So the splitting field for $f(x)$ over F is contained in K. The reverse inclusion is obtained by taking the minimal polynomial for any element in the splitting field and observing that such an element is a root of one of the $m_{\alpha_i}(x)$, meaning it must be in K as assumed. Hence K is a splitting field over F. □

2. (13.4.6) Let K_1 and K_2 be finite extensions of F contained in the field K, and assume both are splitting fields over F.

   (a) Prove that their composite K_1K_2 is a splitting field over F.

Proof. Let K_1 be a splitting field for $f_1(x)$ over F (it is K adjoined with every root of $f_1(x)$) and K_2 be a splitting field for $f_2(x)$ over F (it is K adjoined with every root of $f_2(x)$. Then we show that K_1K_2 is the splitting field for $f(x) = f_1(x)f_2(x)$ over F.

Observe that the splitting field for $f(x)$ is contained in K_1K_2 since K_1K_2 contains all the roots for both $f_1(x)$ and $f_2(x)$ (since K_1K_2 is F adjoined with every root of $f_1(x)$ and $f_2(x)$.), which enables $f_1(x)f_2(x)$ to split completely. The reverse inclusion comes from the fact that in order for $f(x)$ to split completely in a field, it must contain the roots of $f_1(x)$ and $f_2(x)$. So the splitting field contains both K_1 and K_2, and by minimality of the composite field, K_1K_2 is contained in the splitting field. Hence it is the splitting field for $f(x)$. □

(b) Prove that $K_1 \cap K_2$ is a splitting field over F. [Use the preceding exercise.] We show that every irreducible polynomial which has a root in $K_1 \cap K_2$ splits completely. Let $f(x) \in F[x]$ be an irreducible polynomial with a root α in $K_1 \cap K_2$. But because α is in a splitting field K_1 over F and $f(x)$ is irreducible, it splits in $K_1[x]$ so that every root of $f(x)$ is contained in K_1. Similarly, every root of $f(x)$ is contained in K_2, so that every root of $f(x)$ is in $K_1 \cap K_2$. It follows that $f(x)$ splits completely in $(K_1 \cap K_2)[x]$, and since $f(x)$ was an arbitrary irreducible polynomial in $F[x]$, we have that $K_1 \cap K_2$ is a splitting field over F.

3. (13.5.6) Prove that $x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (x - \alpha)$. Conclude that $\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = (-1)^{p^n}$ so the product of the nonzero elements of a finite field is $+1$ if $p = 2$ and -1 if p is odd. For p odd and $n = 1$ derive *Wilson's Theorem*: $(p-1)! \equiv -1 \pmod{p}$.

Proof. Observe that the polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$ is separable since its derivative is -1, and $\gcd(x^{p^n} - x, -1) = 1$, meaning it has exactly p^n roots, all of which are in $\mathbb{F}_{p^n}$. Following the example in the text, it follows that $x^{p^n} - x = \prod_{\alpha \in \mathbb{F}_{p^n}} (x - \alpha)$. By factoring out $(x - 0)$ from both sides we obtain the equality $x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (x - \alpha)$ as desired.

By evaluating both sides of the above equality at $x = 0$, it follows that $\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = -1 = (-1)^{p^n}$ (powers of odd numbers are odd, and when $p = 2$ $-1 = 1$).

Then when p is odd and $n = 1$, we have $-1 = \prod_{\alpha \in \mathbb{F}_p^\times} \alpha = (p-1)!$, which is Wilson's theorem. □

4. (Problem 2) The ring $R = k[\varepsilon]/(\varepsilon^2)$ is called the ring of dual numbers over a field k.

(a) Given a polynomial $f(x) \in k[x]$, show that $f(x + \varepsilon) = f(x) + D_x(f(x))\varepsilon \in R[x]$.

Proof. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be an element of $k[x]$. We find what $f(x + \varepsilon) \in R[x]$ is by

using the binomial theorem and the fact that $\varepsilon^k = 0$ for all $k \geq 2$:

$$\begin{aligned} f(x+\varepsilon) &= a_n(x+\varepsilon)^n + \cdots + a_1(x+\varepsilon) + a_0 \\ &= a_n\left(\sum_{i=0}^{n} \binom{n}{i} x^{n-i}\varepsilon^i\right) + \cdots + (a_1 x + a_1\varepsilon) + a_0 \\ &= (a_n x^n + n a_n x^{n-1}\varepsilon) + \cdots + (a_1 x + a_1\varepsilon) + a_0 \\ &= f(x) + D_x(f(x))\varepsilon \end{aligned}$$

as desired. □

(b) Prove the sum and product rules for formal derivatives.

Proof. Let $f(x), g(x) \in k[x]$, and let $h(x) = f(x) + g(x)$. Then $h(x+\varepsilon) = f(x+\varepsilon) + g(x+\varepsilon) \in R[x]$ is equal to both $f(x)+g(x)+D_x(f(x)+g(x))\varepsilon$ and $f(x)+D_x(f(x))\varepsilon+g(x)+D_x(g(x))\varepsilon$. By cancellation we have $D_x(f(x)+g(x)) = D_x(f(x)) + D_x(g(x))$.

Similarly, let $f(x) = f(x)g(x)$. Then $p(x+\varepsilon) = f(x+\varepsilon)g(x+\varepsilon) \in R[x]$ is equal to both $f(x)g(x) + D_x(f(x)g(x))\varepsilon$ and $(f(x)+D_x(f(x))\varepsilon)(g(x)+D_x(g(x))\varepsilon) = f(x)g(x)+f(x)D_x(g(x))\varepsilon+g(x)D_x(f(x))\varepsilon+ D_x(f(x))D_x(g(x))\varepsilon^2$. Since $\varepsilon^2 = 0$, we have by cancellation that $D_x(f(x)g(x)) = f(x)D_x(g(x)) + g(x)D_x(f(x))$. □

The dual numbers show up when defining the tangent space in algebraic geometry.

Feedback

1. 13.4.5 and 13.5.6 seem like they could use feedback, thanks.

2. I think things are still okay; this homework was slightly more challenging than the previous one but I am grateful for your help in office hours. This was the first time I have come to office hours for anything more serious than asking a professor to sign something or similar and I am happy that it was very chill and not at all scary.

   I noticed that we've been caring more and more about finite fields, and from whatever number theory I remember there were a number of results involving the integers modulo primes or powers of primes, like Wilson's theorem from this homework. Will we continue to see applications to number theory? My guess is there are very powerful applications of field/Galois theory in number theory, which could be cool to see.