Graded

1. (13.6.4) Prove that if $n = p^k m$ where p is a prime and m is relatively prime to p then there are precisely m distinct roots of unity over a field of characteristic p.

   Proof. Let F be a field of characteristic p and let $n = p^k m$ with m relatively prime to p as above. Then the roots of unity are the roots of the polynomial $f(x) = x^n - 1 = x^{p^k m} - 1$. Since $D_x(f(x)) = p^k m x^{p^k m - 1} = 0$, $f(x)$ is inseparable and so we show that there are m distinct roots which are repeated.

   Since F is characteristic p, write $f(x)$ as $(x^m)^{p^k} - 1^{p^k} = (x^m - 1)^{p^k}$, so that the roots which are repeated are indeed the roots of $x^m - 1$. But $x^m - 1$ is separable since its derivative is mx^{m-1} ($\neq 0$ since $p \nmid m$), which shares no roots with $x^m - 1$ (if there were such a root, its minimal polynomial would divide both $x^m - 1$ and mx^{m-1} so that $\gcd(x^m - 1, mx^{m-1}) \neq 0$). Hence $x^m - 1$ carries with it exactly m distinct roots; as a result $f(x)$ does also. □

2. (An Infinite Extension) Let K be a field of characteristic zero. Recall that $K(x)$ is the field of rational functions over K (the field of fractions of $K[x]$).

   (a) Show that $\sigma_n \colon K(x) \to K(x)$ defined by sending x to $x + n$ is an automorphism of $K(x)$.

   Proof. Let $f(x), g(x) \in K(x)$. Then

$$\begin{aligned} \sigma_n(f(x) \pm g(x)) &= f(x+n) \pm g(x+n) \\ &= \sigma_n(f(x)) \pm \sigma_n(g(x)) \\ \sigma(f(x)g(x)) &= f(x+n)g(x+n) \\ &= \sigma_n(f(x))\sigma_n(g(x)), \end{aligned}$$

   and for $g(x)$ not zero,

$$\begin{aligned} \sigma_n(f(x)/g(x)) &= f(x+n)/g(x+n) \\ &= \sigma_n(f(x))/\sigma_n(g(x)). \end{aligned}$$

   Furthermore, $\sigma_{-n} \colon K(x) \to K(x)$ sending x to $x - n$ is a left and right inverse to σ_n. It follows σ_n is an automorphism of $K(x)$ Since K is characteristic zero, each σ_n is not the identity. □

   (b) Let $G = \{\sigma_n \mid n \in \mathbb{Z}\} \subset \mathrm{Aut}(K(x))$. What is the fixed field of G (i.e. what is $K(x)^G$)?
   The fixed field $K(x)^G$ is K.

   Proof. Let $f(x) = p(x)/g(x)$ be an element of $K(x)$ with $p(x), g(x) \in K[x]$ irreducible and coprime with $g(x)$ nonzero. Then for any σ_n, we have $\sigma_n(f(x)) = p(x+n)/g(x+n)$; for $f(x)$ to be in $K(x)^G$, we must have $p(x)/g(x) = p(x+n)/g(x+n)$ for all $n \in \mathbb{Z}$.

   Since $p(x)$ and $g(x)$ are coprime (so that $p(x+n)$ and $g(x+n)$ are also), the rational functions $p(x)/g(x)$ and $p(x+n)/g(x+n)$ are equivalent if the roots of $p(x)$ and $g(x)$ coincide with the roots of $p(x+n)$

and $g(x+n)$, respectively. (Note these polynomials are separable since K is characteristic 0, so we do not need to worry about comparing multiplicities of roots.)

Let α be a root of $p(x)$ and β a root of $g(x)$. For each $n \in \mathbb{Z}$, if σ_n fixes $f(x) = p(x)/g(x)$, then $p(x+n)$ shares the same roots with $p(x)$ and $g(x+n)$ shares the same roots with $g(x)$. Thus for each $n \in \mathbb{Z}$ $\alpha - n$ is a root of $p(x)$ and $\beta - n$ is a root of $g(x)$. With $\alpha \neq \alpha - n$ and $\beta \neq \beta - n$ for each n, we have that $p(x)$ and $g(x)$ have infinitely many roots, which is impossible unless $p(x)$ and $g(x)$ had no roots to begin with. Hence $p(x), g(x)$ are degree 0 and so any element in $K(x)^G$ is of the form k_1/k_2 for $k_1, k_2 \in K$. It follows that $K(x)^G = K$. $\square$

(c) What is $[K(x)\colon K(x)^G]$?

The degree of $K(x)$ over $K(x)^G = K$ is infinite.

Proof. Since $K(x)$ is a field extension of K, we have that $K(x)$ is a K-vector space. To show that the basis is not finite, we exhibit an infinite set of linearly independent elements of $K(x)$ over K: consider $\{x^n \mid n \in \mathbb{Z}\}$; this is one such infinite linearly independent set. Hence the basis contains at least infinitely many elements, meaning the degree of the extension $K(x)$ over $K(x)^G = K$ is not finite. $\square$

Additional Problems

1. (13.5.2) Find all irreducible polynomials of degrees 1, 2 and 4 over $\mathbb{F}_2$ and prove that their product is $x^{16} - x$.

Proof. It is clear that the degree 1 irreducible polynomials in $\mathbb{F}_2[x]$ are x, $x+1$.

The degree 2 polynomials are of the form $x^2 + a_1x + a_0$; to be irreducible a_0 must be 1 and from there it follows that a_1 must be 1 so that $x^2 + x + 1$ is the only degree 2 polynomial with no roots in $\mathbb{F}_2$.

Degree 4 polynomials are of the form $x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$; to be irreducible, we first demand a_0 be 1. Then we would not want 1 to be a root of such a polynomial, so we need there to be an odd number of terms (so two of a_3, a_2, a_1 must be zero or they are all 1). Further note that $x^4 + x^2 + 1 = x^4 + 2x^3 + 3x^2 + 2x + 1 = (x^2 + x + 1)^2$ is not irreducible.

We check that the only remaining polynomials $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$, and $x^4 + x + 1$ are irreducible by seeing that $x^2 + x + 1$ does not divide any of these three (by long division in $\mathbb{F}_2[x]$). Hence the above are the only irreducible degree 4 polynomials.

Computing, we have

$$
\begin{aligned}
&(x)[(x+1)(x^4+x^3+x^2+x+1)](x^2+x+1)[(x^4+x+1)(x^4+x^3+1)] \\
=&(x)(x^5+1)[(x^2+x+1)(x^8+x^7+x^5+x^4+x^3+x+1)] \\
=&(x)[(x^5+1)(x^{10}+x^5+1)] \\
=&(x)(x^{15}+1) \\
=&\ x^{16}+x
\end{aligned}
$$

as desired. □

2. (13.5.9) Show that the binomial coefficient $\binom{pn}{pi}$ is the coefficient of x^{pi} in the expansion of $(1+x)^{pn}$. Working over $\mathbb{F}_p$ show that this is the coefficient of $(x^p)^i$ in $(1+x^p)^n$ and hence prove that $\binom{pn}{pi} \equiv \binom{n}{i} \pmod{p}$.

   Proof. By the binomial theorem, $(1+x)^{pn} = \sum_{k=0}^{pn} \binom{pn}{k} x^k$ so that the coefficient of x^{pi} is $\binom{pn}{pi}$ as expected. Working in $\mathbb{F}_p$, we write $(1+x)^{pn}$ as $[(1+x)^p]^n = (1^p + x^p)^n = (1+x^p)^n = \sum_{k=0}^{n} \binom{n}{k}(x^p)^k$ so that the coefficient for $x^{pi} = (x^p)^i$ is $\binom{n}{i}$. Since both binomial expansions are valid for $(1+x)^{pn}$ in $\mathbb{F}_p$ it follows that $\binom{pn}{pi} \equiv \binom{n}{i} \pmod{p}$. □

3. (13.6.6) Prove that for n odd, $n > 1$, $\Phi_{2n}(x) = \Phi_n(-x)$.

   Proof. Observe that $\Phi_{2n}(x)$ is the minimal polynomial for any $2n$-th root of unity. Note also that $\Phi_n(x)$ is a minimal polynomial, so that $\Phi_n(-x)$ is irreducible also; it is also monic since its degree is $\varphi(n)$, which for odd $n > 1$ will be even since φ is even for prime powers. Hence both polynomials $\Phi_{2n}(x), \Phi_n(-x)$ are minimal polynomials over any of its roots. If they share a common root, they must be equal by uniqueness of the minimal polynomial.

   Claim: $\zeta_2\zeta_n = -\zeta_n$ is a common root: Clearly it is a root of $\Phi_n(-x)$, but to see that it is a root of $\Phi_{2n}(x)$ we show that $-\zeta_n$ has order $2n$ in the group of $2n$-th roots of unity. Observe that $(-\zeta_n)^{2n} = \zeta_n^{2n} = 1$ so that the order of $-\zeta_n$ divides $2n$. But the order of -1 is 2 and the order of ζ_n is n, and since $\gcd(2,n) = 1$ it follows that the order of their product cannot be any lower than $2n$; that is, it must be exactly $2n$ as desired. Hence $-\zeta_n$ is a common root of the above two minimal polynomials so they must be equivalent. □

4. (13.6.8) Let ℓ be a prime and let $\Phi_\ell(x) = \frac{x^\ell - 1}{x-1} = x^{\ell-1} + x^{\ell-2} + \cdots + x + 1 \in \mathbb{Z}[x]$ be the ℓ^{th} cyclotomic polynomial, which is irreducible by Theorem 41. This exercise determines the factorization of $\Phi_\ell(x)$ modulo p for any prime p. Let ζ denote any fixed primitive ℓ^{th} root of unity.

   (a) Show that if $p = \ell$ then $\Phi_\ell(x) = (x-1)^{\ell-1} \in \mathbb{F}_\ell[x]$.

   Proof. In $\mathbb{F}_\ell[x]$, write $x^\ell - 1$ as $(x-1)^\ell$ so that $\Phi_\ell(x) = \frac{x^\ell-1}{x-1} = \frac{(x-1)^\ell}{x-1} = (x-1)^{\ell-1}$ as desired. □

   (b) Suppose $p \neq \ell$ and let f denote the order of p mod ℓ, i.e., f is the smallest power of p with $p^f \equiv 1$ mod ℓ. Use the fact that $\mathbb{F}_{p^n}^\times$ is a cyclic group to show that $n = f$ is the smallest power p^n of p with $\zeta \in \mathbb{F}_{p^n}$. Conclude that the minimal polynomial of ζ over $\mathbb{F}_p$ has degree f.

   Proof. We show that ζ satisfies $x^{p^f-1} - 1$ in $\mathbb{F}_{p^f}^\times$: since $p^f \equiv 1 \pmod{\ell}$, it follows that there is an integer $m \geq 1$ such that $p^f - 1 = m\ell$. Then $\zeta^{p^f-1} - 1 = \zeta^{m\ell} - 1 = 1^m - 1 = 0$ as desired. No smaller power p^n will admit this inclusion: if $n < f$, then $p^n \not\equiv 1 \pmod{\ell}$ so that $p^n - 1 = m\ell + r$ for $0 < r < \ell$. Then $\zeta^{p^n-1} - 1 = \zeta^{m\ell+r} - 1 = \zeta^r - 1 \neq 0$.

   Since $\mathbb{F}_{p^f}$ is a degree f extension of $\mathbb{F}_p$ and $\zeta \in \mathbb{F}_{p^f}$, it follows that the minimal polynomial of ζ over $\mathbb{F}_p$ is degree f. □

(c) Show that $\mathbb{F}_p(\zeta) = \mathbb{F}_p(\zeta^a)$ for any integer a not divisible by ℓ. [One inclusion is obvious. For the other, note that $\zeta = (\zeta^a)^b$ where b is the multiplicative inverse of a mod ℓ.] Conclude using (b) that, in $\mathbb{F}_p[x]$, $\Phi_\ell(x)$ is the product of $\frac{\ell-1}{f}$ distinct irreducible polynomials of degree f.

Proof. The inclusion $\mathbb{F}_p(\zeta^a) \subseteq \mathbb{F}_p(\zeta)$ is clear since ζ^a is a power of ζ. The reverse inclusion is shown similarly, that ζ is a power of ζ^a. The power desired is the multiplicative inverse of a viewed as an element of $\mathbb{F}_\ell^\times$ (recall ℓ is prime and $\gcd(a, \ell) = 1$). Call this multiplicative inverse b so that $(\zeta^a)^b = \zeta^{ab} = \zeta^{1+m\ell} = \zeta$ for some integer m; it follows that ζ is a power of ζ^a so that the reverse inclusion holds.

Since the minimal polynomial of ζ over $\mathbb{F}_p$ has degree f it follows that $\mathbb{F}_{p^f} = \mathbb{F}_p(\zeta) = \mathbb{F}_p(\zeta^a)$ for $1 \leq a \leq \ell - 1$. But each of the $\ell - 1$ roots ζ^a are roots of $\Phi_\ell(x)$ viewed as an element of $\mathbb{F}_p$, so each of their minimal polynomials (and hence their product) divides $\Phi_\ell(x)$. In fact since $\Phi_\ell(x)$ is separable (it has no repeated roots so we consider degrees) and has degree $\ell - 1$, it follows that it has exactly $\frac{\ell-1}{f}$ distinct irreducible factors over $\mathbb{F}_p$ of degree f. □

(d) In particular, prove that, viewed in $\mathbb{F}_p[x]$, $\Phi_7(x) = x^6 + x^5 + \cdots + x + 1$ is $(x+1)^6$ for $p = 7$, a product of distinct linear factors for $p \equiv 1$ mod 7, a product of 3 irreducible quadratics for $p \equiv 6$ mod 7, a product of 2 irreducible cubics for $p \equiv 2, 4$ mod 7, and is irreducible for $p \equiv 3, 5$ mod 7.

Proof. Use part (a) to see that $\Phi_7(x) = \frac{x^7-1}{x-1} = (x+1)^6 \in \mathbb{F}_7[x]$. When $p \equiv 1 \pmod 7$, p has order 1 so that by the formula in (c), $\Phi_7(x)$ is the product of $(7-1)/1 = 6$ degree 1 factors. Similarly, the order of 6 is 2, the order of 2 and 4 is 3, and the order of 3 and 5 is 6.

Therefore:

When $p \equiv 6 \pmod 7$, $\Phi_7(x)$ is the product of $(7-1)/2 = 3$ degree 2 factors.

When $p \equiv 6 \pmod 7$, $\Phi_7(x)$ is the product of $(7-1)/2 = 3$ degree 2 factors.

When $p \equiv 2, 4 \pmod 7$, $\Phi_7(x)$ is the product of $(7-1)/3 = 2$ degree 3 factors.

When $p \equiv 3, 5 \pmod 7$, $\Phi_7(x)$ is the product of $(7-1)/6 = 1$ degree 6 factor (i.e. it is irreducible). □

5. (14.1.1)

(a) Show that if the field K is generated over F by the elements $\alpha_1, \ldots, \alpha_n$ then an automorphism σ of K fixing F is uniquely determined by $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$. In particular show that an automorphism fixes K if and only if it fixes a set of generators for K.

Proof. Let σ be an automorphism of $K = F(\alpha_1, \ldots, \alpha_n)$ which fixes F. Any element of K is of the form $k = f(\alpha_1, \ldots, \alpha_n)/g(\alpha_1, \ldots, \alpha_n)$ for polynomials f, g. Since σ is an automorphism that fixes F it follows that $\sigma(k) = f(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))/g(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$. Hence the action of σ is determined by its action on each α_i; that is, σ_1 agrees with σ_2 if and only if for every k in the above form, $\sigma_1(k) = \sigma_2(k)$ – if and only if each automorphism agrees on each α_i.

In particular it follows that σ above is the identity map on K if $\sigma(\alpha_i) = \alpha_i$ for each i. □

(b) Let $G \leq \mathrm{Gal}(K/F)$ be a subgroup of the Galois group of the extension K/F and suppose $\sigma_1, \dots, \sigma_k$ are generators for G. Show that the subfield E/F is fixed by G if and only if it is fixed by the generators $\sigma_1, \dots, \sigma_k$.

Proof. Since K is Galois over F, it is a finite extension; hence E is also. Let $E = F(\alpha_1, \dots, \alpha_n)$.

Suppose E/F is fixed by each of the generators $\sigma_1, \dots, \sigma_k$ for G. It follows that every automorphism $\sigma \in G$ fixes E/F since σ may be represented as a finite product (compositions) of the σ_i, and each of those fix E/F.

Conversely, suppose G fixes E/F; it follows immediately that $\sigma_i \in G$ fix E/F. $\square$

6. (14.1.7) This exercise determines $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$.

(a) Prove that any $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ takes squares to squares and takes positive reals to positive reals. Conclude that $a < b$ implies $\sigma a < \sigma b$ for every $a, b \in \mathbb{R}$.

Proof. Since σ is an automorphism, if $s = r^2$ for $r \in \mathbb{R}$ is a square of a real number then $\sigma(s) = \sigma(r^2) = \sigma(r)^2$ and $\sigma(r) \in \mathbb{R}$ as desired. In particular every positive real number is the square of some real number, so every positive real number is sent to a positive real number.

Then if $a, b \in \mathbb{R}$ with $0 < b - a$ then $0 < \sigma(b-a) = \sigma(b) - \sigma(a)$, so σ is order preserving. $\square$

(b) Prove that $-\frac{1}{m} < a - b < \frac{1}{m}$ implies $-\frac{1}{m} < \sigma a - \sigma b < \frac{1}{m}$ for every positive integer m. Conclude that σ is a continuous map on $\mathbb{R}$.

Proof. For any positive integer m if $-\frac{1}{m} < a - b < \frac{1}{m}$, then since σ fixes $\mathbb{Q}$ and is order preserving, it follows that $\sigma\left(-\frac{1}{m}\right) = -\frac{1}{m} < \sigma(a-b) = \sigma(a) - \sigma(b) < \frac{1}{m} = \sigma\left(\frac{1}{m}\right)$.

We show that σ is continuous at every real number r. Let $\varepsilon > 0$ be given, and choose m large enough so that $\frac{1}{m} < \varepsilon$. If $|x - r| < \frac{1}{m}$, then by the above argument $|\sigma(x) - \sigma(r)| < \frac{1}{m} < \varepsilon$ so that σ is continuous at r. Since r was arbitrary, σ is continuous on $\mathbb{R}$. $\square$

(c) Prove that any continuous map on $\mathbb{R}$ which is the identity on $\mathbb{Q}$ is the identity map, hence $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = 1$.

Proof. Let r be any real number. Then since $\mathbb{R}$ is a complete space, there is a (Cauchy) sequence (a_n) converging to r from $\mathbb{Q}$. Since any $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ is continuous, it preserves convergence of the sequence (a_n) in that $(\sigma(a_n))$ converges to $\sigma(r)$. But σ fixes $\mathbb{Q}$ so that $(\sigma(a_n)) = (a_n)$; hence $\sigma(r) = r$. It follows that every σ agrees with the identity map, so $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = 1$. $\square$

Feedback

1. 14.1.7, thanks.

2. Things are okay as usual; just eager to learn more Galois theory because it has been a while since I thought about groups like symmetric groups or automorphism groups. It's nice to see things return like that.