Kris Harper
MATH 25900
Homework 3 — April 23, 2010

Problem 1 (13.4.1). *Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 - 2$.*

Proof. If α is a root of this polynomial then $(\zeta\alpha)^4 = 2$ where ζ is fourth root of unity so the four solutions are $\zeta^n \sqrt[4]{2}$ where $1 \leq n \leq 4$. Note that the splitting field for this polynomial must then contain $\mathbb{Q}(\zeta, \sqrt[4]{2})$ and this extension also contains all the roots, so the splitting field must be $\mathbb{Q}(\zeta, \sqrt[4]{2})$. This field contains the extension $\mathbb{Q}(\zeta)$ and is generated over it by $\sqrt[4]{2}$ so we must have $[\mathbb{Q}(\zeta, \sqrt[4]{2}), \mathbb{Q}] = 4\phi(4) = 8$. $\square$

Problem 2 (13.4.2). *Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 + 2$.*

Proof. This follows the exact same argument as Problem 1 but with $\sqrt[4]{-2}$ in place of $\sqrt[4]{2}$. We then have the splitting field $\mathbb{Q}(\zeta, \sqrt[4]{-2})$ with extension degree 8. $\square$

Problem 3 (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.
(b) Prove that $K_1 \cap K_2$ is a splitting field over F.

Proof. (a) Let $f(x)$ and $g(x)$ be the polynomials for which K_1 and K_2 are respectively splitting fields. Note that $f(x)g(x)$ splits completely in K_1K_2 and this is the smallest field extension containing both K_1 and K_2. Since K_1 and K_2 are the smallest fields for which $f(x)$ and $g(x)$ split completely it follows that K_1K_2 must be the splitting field for $f(x)g(x)$.

(b) Let $f(x)$ be an irreducible polynomial in $F[x]$ with a root in $K_1 \cap K_2$. Then $f(x)$ has a root in K_1 and a root in K_2 so it splits completely in these two fields since they are splitting fields. But then the factors $f(x)$ splits into are contained in both K_1 and K_2 so $f(x)$ splits completely in $K_1 \cap K_2$ as well. Thus $K_1 \cap K_2$ is a splitting field for F. $\square$

Problem 4 (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. Degrees 1 and 2 are easily taken care of. The polynomials x and $x+1$ are irreducible of degree 1 and the only such. The polynomial x^2+x+1 is the only irreducible polynomial of degree 2 as $x^2+x = x(x+1)$, $x^2 = xx$ and $x^2+1 = (x+1)^2$.

There are 16 polynomials of degree 4 in $\mathbb{F}_2[x]$. If the constant term is 0 then we can factor x out so this reduces the number to 8. We now have

$$\begin{aligned} x^4+x^3+x^2+1 &= (x+1)(x^3+x+1) \\ x^4+x^3+x+1 &= (x+1)^2(x^2+x+1) \\ x^4+x^2+x+1 &= (x+1)(x^3+x^2+1) \\ x^4+x^2+1 &= (x^2+x+1)^2 \\ x^4+1 &= (x+1)^4 \end{aligned}$$

We are left with the three polynomials x^4+x+1, x^4+x^3+1 and $x^4+x^3+x^2+x+1$. Putting in 0 and 1 immediately shows that none of these polynomials has a linear factor. Consider the product of the two quadratics $(x^2+ax+1)(x^2+bx+1)$. But now note that the cases where $a = b = 1$, $a = 0$, $b = 1$ and $a = b = 0$ are all covered in the factorizations above. Thus these three polynomials are irreducible. Taking the product of these three polynomials as well as x^2+x+1, $x-1$ and x gives $x^{16} - x$. $\square$

Problem 5 (13.5.3). *Prove that d divides n if and only if $x^d - 1$ divides $x^n - 1$.*

Proof. Suppose $d \mid n$ and let $d' = n/d$. Then $(x^d-1)(1+x^d+x^{2d}+\cdots+x^{(d'-1)d}) = x^{dd'} - 1 = x^n - 1$. Conversely suppose $x^d - 1 \mid x^n - 1$ so that $x^n - 1 = (x^d-1)f(x)$. Write $n = qd + r$ so that $(x^d-1)f(x) = x^n - 1 = (x^{qd+r} - x^r) + (x^r - 1) = x^r(x^{qd}-1) + (x^r-1)$. Since $x^d - 1$ divides the left hand of this equation and divides $x^{qd-1} - 1$ (since $d \mid qd$) we see that it must also divide $x^r - 1$. But $r < d$ so $r = 0$ and $n = qd$. $\square$

Kris Harper
MATH 25900
Homework 3 April 23, 2010

Problem 6 (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 $\mathbb{F}_p$.*

Proof. Suppose $x^p - x + a = (x^n + \cdots + b)(x^m + \cdots + c)$ with n and m nonzero. Using the product rule for derivatives, the derivative of the right side is $(nx^{n-1} + \cdots + b')(x^m + \cdots + c) + (mx^{m-1} + \cdots + c')(x^n + \cdots + b)$. Since m and n are both positive and nonzero we see that this polynomial must have degree x^{m+n-1}, but the derivative of the left hand side is -1. This is a contradiction and so $x^p - x + a$ must be irreducible. Since irreducible polynomials in a finite field are separable we must have $x^p - x + a$ is also separable. $\square$

Problem 7 (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. Note that if $\alpha \in \mathbb{F}_{p^n}^\times$ then $\alpha^{p^n-1} = 1$. Consider the polynomial $f(x) = (x^{p^n-1} - 1) - \prod_{\alpha \in \mathbb{F}_{p^n}^\times}(x - \alpha)$. This has $p^n - 1$ roots, but degree less than $p^n - 1$, thus it must be identically 0. If we set $x = 0$ in the above formula then we have $-1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times}(-\alpha) = (-1)^{p^n-1}\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha$ so $\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = -(-1)^{-p^n+1} = -((-1)^{p^n-1})^{-1} = (-1)^{p^n}$. When $n = 1$ we have $\prod_{\alpha \in \mathbb{F}_p^\times} \alpha = (-1)^p$. Reducing this equation modulo p we get $(p-1)! \equiv -1 \pmod p$. Note that the right hand side is clearly -1 for p odd, and is easily verified for $p = 2$ since $1 \equiv -1 \pmod 2$. $\square$

Problem 8 (13.6.2)**.** *Let ζ_n be a primitive n^{th} root of unity and let d be a divisor of n. Prove that ζ_n^d is a primitive $(n/d)^{\text{th}}$ root of unity.*

Proof. Let m be the order of ζ_n^d so that $(\zeta_n^d)^m = \zeta_n^{md} = 1$. Since ζ_n is an n^{th} root of unity we see that $n \mid md$ and since m is minimal we must have $m = n/d$. Therefore ζ_n^d is a primitive $(n/d)^{\text{th}}$ root of unity. $\square$

Problem 9 (13.6.7)**.** *Use the Möbius Inversion formula indicated in Section 14.3 to prove*

$$\Phi_m(x) = \prod_{d \mid m}(x^d - 1)^{\mu(m/d)}.$$

Proof. We know $x^m - 1 = \prod_{d \mid m}\Phi_d(x)$. The Möbius inversion formula tells us that we can recover $\Phi_m(x)$ as $\Phi_m(x) = \prod_{d \mid m}(x^{m/d} - 1)^{\mu(d)}$. Changing the index to $d' = m/d$ gives us the desired result. $\square$

Problem 10 (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 over $\mathbb{Z}$ 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 $\Phi_\ell(x) = (x-1)^{\ell-1} \in \mathbb{F}_\ell[x]$.
(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 $p^f \equiv 1 \pmod \ell$. 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.
(c) Show that $\mathbb{F}_p(\zeta) = \mathbb{F}_p(\zeta^a)$ for any integer a not divisible by 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.
(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 $p \equiv 1 \pmod 7$, a product of 3 irreducible quadratics for $p \equiv 6 \pmod 7$, a product of 2 irreducible cubics for $p \equiv 2, 4 \pmod 7$, and is irreducible for $p \equiv 3, 5 \pmod 7$.

Proof. (a) Over $\mathbb{F}_\ell$ we know $x^\ell - 1 = (x-1)^\ell$ so $\Phi_\ell(x) = (x-1)^\ell/(x-1) = (x-1)^{\ell-1}$.

(b) Suppose ζ is an ℓ^{th} root of unity in the extension $\mathbb{F}_{p^n}$. Then ζ has order ℓ in $\mathbb{F}_{p^n}$ and $\ell \mid p^n - 1$. Thus $p^n \equiv 1 \pmod \ell$. On the other hand, suppose $p^n \equiv 1 \pmod \ell$ so that $\ell \mid p^n - 1$. Since $\mathbb{F}_{p^n}^\times$ is cyclic there exists some element of order ℓ in $\mathbb{F}_{p^n}$. Thus $\zeta \in \mathbb{F}_{p^n}$ if and only if $p^n \equiv 1 \pmod l$ which is true if and only if $f \mid n$. Thus f is the smallest such integer for which this is true. The smallest extension over $\mathbb{F}_p$ containing ζ then must have degree f so this is the degree of it's minimal polynomial.

(c) It's clear that $\mathbb{F}_p(\zeta^a) \subseteq \mathbb{F}_p(\zeta)$ since fields are closed under multiplication. Noting that $\zeta = (\zeta^a)^b$ with $ab \equiv 1 \pmod{\ell}$ we see that $\mathbb{F}_p(\zeta) \subseteq \mathbb{F}_p(\zeta^a)$.

For $(a, \ell) = 1$ we know ζ^a encompasses all the primitive roots modulo ℓ so $\mathbb{F}_p(\zeta) = \mathbb{F}_{p^f}$ is the unique extension of $\mathbb{F}_p$ of degree f which contains all primitive roots modulo ℓ. We then know the minimal polynomial for ζ^a is of degree f as well so $\Phi_\ell(x) = m_1(x) \dots m_k(x)$ where $k = (\ell - 1)/f$ since each $m_i(x)$ has degree f. We know each m_i is distinct because $\Phi_\ell(x)$ is separable over $\mathbb{F}_p$ for $p \neq \ell$.

(d) Part (a) tells us that $\Phi_7(x) = (x-1)^6$ in $\mathbb{F}_7$. We can now compute f for the various cases. If $p \equiv 1 \pmod 7$ then $f = 1$ so $\Phi_7(x)$ splits into $(7-1)/1 = 6$ linear factors. If $p \equiv 6 \pmod 7$ then $f = 2$ so $\Phi_7(x)$ splits into $(7-1)/2 = 3$ quadratics. If $p \equiv 2 \pmod 7$ or $p \equiv 4 \pmod 7$ then $f = 3$ so $\Phi_7(x)$ splits into $(7-1)/3 = 2$ cubics. And if $p \equiv 3 \pmod 7$ or $p \equiv 5 \pmod 7$ then $f = 6$ so $\Phi_7(x)$ is irreducible. □

Problem 11 (14.1.4). *Prove that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.*

Proof. We know $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ so the Galois group for this extension cannot have order larger than 4. But the automorphisms taking $\sqrt{2}$ to $-\sqrt{2}$ and $\sqrt{3}$ to $-\sqrt{3}$ already enumerate 4 maps. Thus there is no automorphism taking $\sqrt{2}$ to $\sqrt{3}$ so the two fields cannot be isomorphic. □

Problem 12 (14.1.6). *Let k be a field.*
(a) Show that the mapping $\varphi : k[t] \to k[t]$ defined by $\varphi(f(t)) = f(at+b)$ for fixed $a, b \in k$, $a \neq 0$ is an automorphism of $k[t]$ which is the identity on k.
(b) Conversely, let φ be an automorphism of $k[t]$ which is the identity on k. Prove that there exist $a, b \in k$ with $a \neq 0$ such that $\varphi(f(t)) = f(at+b)$ as in (a).

Proof. (a) Let $f(t), g(t) \in k[t]$. Then $\varphi(f(t) + g(t)) = f(at+b) + g(at+b) = \varphi(f(t)) + \varphi(g(t))$ and $\varphi(f(t)g(t)) = f(at+b)g(at+b) = \varphi(f(t))\varphi(g(t))$ so φ is a homomorphism. Note that φ clearly fixes k because if $f(t)$ is a constant function then $f(at+b)$ is the same constant function.

Now suppose $p(t) = c_n t^n + \cdots + c_0$ and $q(t) = d_m t^m + \cdots + d_0$ distinct elements of $k[t]$. If $p(x)$ and $q(x)$ have different degrees then their images are clearly distinct. Otherwise let i be the largest index such that $c_i \neq d_i$. Then $\varphi(p(t))$ has the term $c_i(at+b)^i$ while $\varphi(q(t))$ has the term $d_i(at+b)^i$. Since the polynomials are identical for indices greater than i there is no cancellation of the terms $c_i a t^i \neq d_i a t^i$. Thus $\varphi(p(t)) \neq \varphi(q(t))$ and φ is injective.

Finally consider the polynomial $c'_n(at+b)^n + \cdots + c'_0$. If we expand this out and compare degrees with $p(t)$ we can recursively solve for the c'_i in terms of the c_i. That is, first solve for c'_n in terms of c_n, a and b, then solve for c'_{n-1} in terms of c_n, c_{n-1}, a and b. Continue in this way until we can rewrite $c'_n(at+b)^n + \cdots + c_0$ in terms of c_i, a and b. But then applying φ to this polynomial will give back $p(t)$ so φ is surjective as well.

(b) Now suppose φ is an automorphism of $k[t]$ fixing k. Let $f(t) = c_n t^n + \cdots + c_0$ be any element of $k[t]$. Note that $\varphi(f(t)) = \varphi(c_n t^n) + \cdots + \varphi(c_0) = c_n \varphi(t^n) + \cdots + c_0$ since φ is a homomorphism fixing k. Thus φ is completely determined by which polynomial it sends t to. Note that $\deg \varphi(t) \leq 1$ since, for example, we cannot have $\varphi(t) = t^2 = \varphi(t)\varphi(t)$ so that $t^2 = 1$. On the other hand $\varphi(t) \neq c$ some constant because then φ is clearly not surjective onto $k[t]$. Thus $\varphi(t) = at + b$ with $a \neq 0$ so that $\varphi(f(t)) = f(at+b)$ for some $a, b \in k$. □

Problem 13 (14.1.10). *Let K be an extension of the field F. Let $\varphi : K \to K'$ be an isomorphism of K with a field K' which maps F to the subfield F' of K'. Prove that the map $\sigma \mapsto \varphi\sigma\varphi^{-1}$ defines a group isomorphism $\mathrm{Aut}(K/F) \to \mathrm{Aut}(K'/F')$.*

Proof. Let $\sigma \in \mathrm{Aut}(K/F)$ and $x, y \in K'$. Then $\varphi(\sigma(\varphi^{-1}(x+y))) = \varphi(\sigma(\varphi^{-1}(x) + \varphi^{-1}(y))) = \varphi(\sigma(\varphi^{-1}(x)) + \sigma(\varphi^{-1}(y))) = \varphi(\sigma(\varphi^{-1}(x))) + \varphi(\sigma(\varphi^{-1}(y)))$ so this map is a homomorphism. Furthermore the map is injective and surjective since it's the composition of injective and surjective maps. Thus $\varphi\sigma\varphi^{-1}$ is an element of $\mathrm{Aut}(K'/F')$.

Kris Harper
MATH 25900
Homework 3 April 23, 2010

Let $\sigma, \sigma' \in \mathrm{Aut}(K/F)$ so that $\varphi(\sigma\sigma')\varphi^{-1} = \varphi\sigma\varphi^{-1}\varphi\sigma'\varphi^{-1}$ and the map is a homomorphism. Suppose $\sigma \neq \sigma'$ such that $\sigma(x) \neq \sigma'(x)$ for some $x \in K$. Let $y = \varphi(x)$. Then since φ is injective $\varphi\sigma\varphi^{-1}(y) = \varphi\sigma(x) \neq \varphi\sigma'(x) = \varphi\sigma'\varphi^{-1}(y)$ so the map is injective.

Let $\tau \in \mathrm{Aut}(K'/F')$. Then we've already seen $\varphi^{-1}\tau\varphi$ gives an element $\sigma \in \mathrm{Aut}(K/F)$. But then multiplying on the left by φ and on the right by φ^{-1} gives $\varphi\sigma\varphi^{-1} = \tau$ so the map is surjective and thus an isomorphism. $\square$