MATH 7211 Homework 4

Andrea Bourque

May 9, 2023

1 Problem 13.4.5

Let K/F be a finite extension. Prove that K is a splitting field of a polynomial over F if and only if every irreducible polynomial in $F[x]$ that has a root in K splits in $K[x]$.

Proof. Let K be a splitting field of a polynomial $f(x) \in F[x]$. Since K/F is finite and hence algebraic, there is an algebraic closure of F which contains K, which we denote by $\bar{F}$. Without loss of generality, assume $f(x)$ is monic. Let $K = F(\alpha_1, ..., \alpha_n)$, where the roots of $f(x)$ are $\alpha_1, ..., \alpha_n$ (possibly with repetition). Let $p(x) \in F[x]$ be irreducible with root $\beta \in K$. Let $\gamma \in \bar{F}$ be another root of $p(x)$. By Theorem 8 in Dummit and Foote Chapter 13, there is an isomorphism $F(\beta) \to F(\gamma)$ extending the identity $F \to F$. Let K' be a splitting field of $f(x)$ over $F(\gamma)$, taken to also be contained in $\bar{F}$. By Theorem 27 in Dummit and Foote Chapter 13, there is an isomorphism $\phi : K \to K'$ extending the isomorphism $F(\beta) \to F(\gamma)$. Since ϕ also extends the identity on F, it must fix $f(x)$. Therefore, it must permute the roots α_i of $f(x)$, which are the generators of K. That is, $\phi(K)$ must be exactly K. Since K' contains γ, this means K contains γ as well. Since γ was chosen arbitrarily, it follows that K contains every root of $p(x)$, i.e. $p(x)$ splits over K.

Conversely, suppose every irreducible polynomial in $F[x]$ that has a root in K splits in $K[x]$. Since K/F is a finite extension, we may write $K = F(\alpha_1, ..., \alpha_n)$ for some elements $\alpha_1, ..., \alpha_n \in K$. By hypothesis, each minimal polynomial $m_{\alpha_i,F}(x)$ splits in $K[x]$. Then K contains the splitting field of $f(x) = \prod_i m_{\alpha_i,F}(x)$. But the splitting field of $f(x)$ is generated by the roots of $f(x)$, which are all in K, so the splitting field is contained in K. Thus K is exactly equal to the splitting field of $f(x)$ over F. $\square$

2 Problem 13.5.4

Let a, d, n be positive integers, with $a > 1$. Prove that d divides n if and only if $a^d - 1$ divides $a^n - 1$. Conclude that $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ if and only if d divides n.

Proof. First suppose $n = dk$ for a positive integer k. Then

$$a^n - 1 = (a^d)^k - 1^k = (a^d - 1)(a^{d(k-1)} + ... + 1),$$

so $a^d - 1$ divides $a^n - 1$. Conversely, suppose $a^d - 1$ divides $a^n - 1$. Write $n = qd + r$ with $r < d$. Then $a^n - 1 = a^r(a^{qd} - 1) + a^r - 1$. By the previous analysis, $a^d - 1$ divides $a^{qd} - 1$ and hence $a^r(a^{qd} - 1)$. Thus $a^d - 1$ must divide $a^r - 1$. But $r < d$, so $a^r - 1 < a^d - 1$, since $a > 1$. The only way a positive integer can divide a non-negative integer less than it is if the smaller integer is 0. Thus $a^r - 1 = 0$, so $r = 0$, so $n = qd$, so d divides divides n.

Recall that $\mathbb{F}_{p^k}$ is the splitting field of $x^{p^k - 1} - 1$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (shown in Dummit and Foote, Section 13.5). Then $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ if and only if all the roots of $x^{p^d - 1} - 1$ are roots of $x^{p^n} - 1$, i.e. $x^{p^d - 1} - 1$ divides $x^{p^n - 1} - 1$. By Dummit and Foote exercise 13.5.3, this is equivalent to $p^d - 1$ dividing $p^n - 1$. By the previous work in this exercise, this is equivalent to d dividing n. $\square$

3 Problem 13.5.6

Prove that $x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (x - \alpha)$. Conclude that $\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = (-1)^{p^n}$. For $p > 2$ and $n = 1$, conclude that $(p-1)! \equiv -1 \mod p$.

Proof. As noted in Dummit and Foote section 13.5, the p^n elements of $\mathbb{F}_{p^n}$ are exactly the distinct roots of $x^{p^n} - x$. Removing the factor of x corresponding to the root of 0, we get the factorization in the problem statement.

Substituting $x = 0$ into the factorization gives $-1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (-\alpha)$. Since $F_{p^n}^\times$ has $p^n - 1$ elements, $\prod_{\alpha \in \mathbb{F}_{p^n}^\times} (-\alpha) = (-1)^{p^n-1} \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha$. Multiplying both sides by $(-1)^{p^n-1}$ gives the second desired result.

Finally, when $n = 1$ we have $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, so the non-zero elements are $\{1 \mod p, ..., p-1 \mod p\}$. Thus for p odd we have $\prod_{\alpha \in \mathbb{F}_p^\times} \alpha = -1$, or $(p-1)! \equiv -1 \mod p$. $\square$

4 Problem 13.5.8

Prove that $f(x)^p = f(x^p)$ for any polynomial $f(x) \in \mathbb{F}_p[x]$.

Proof. We induct on the degree of $f(x)$. For $f(x)$ constant, the statement is that $a^p = a$ for any $a \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, which is the statement of Fermat's little theorem. Thus let $f(x) = ax^n + g(x)$, where $a \in \mathbb{F}_p$ and $g(x) \in \mathbb{F}_p[x]$ has degree strictly less than n. Then

$$\begin{aligned} f(x)^p = (ax^n + g(x))^p &= a^p(x^n)^p + g(x)^p \\ &= a(x^p)^n + g(x^p) = f(x^p) \end{aligned}$$

as desired. $\square$

5 Problem 13.6.4

Prove that if $n = p^k m$ where p is a prime not dividing m, then there are precisely m distinct nth roots of unity over a field of characteristic p.

Proof. First suppose p does not divide n, i.e. $k = 0$. Then $x^n - 1$ is seperable over a field of characteristic p, since its derivative nx^{n-1} is nonzero has can only have roots at $x = 0$, which is not a root of $x^n - 1$. Thus the n nth roots of unity are all distinct by Proposition 33 in section 13.5 of Dummit and Foote.

Recall that in a field of characteristic p, we have $(x + y)^p = x^p + y^p$ for any field elements x, y. Applying this equation k times gives $(x + y)^{p^k} = x^{p^k} + y^{p^k}$. Also, note that in a field of characteristic two, $1 = -1$. Then the equation $-1 = (-1)^{p^k}$ is true in a field of characteristic p, regardless of whether p is even or odd.

Now, for $n = p^k m$ as in the statement of the problem, we have

$$x^n - 1 = (x^m)^{p^k} - 1^{p^k} = (x^m - 1)^{p^k}.$$

Thus if $x^n - 1 = 0$, we must have $x^m - 1 = 0$. Since p does not divide m, our earlier work shows that there are m distinct solutions to $x^m - 1 = 0$. Therefore, these m distinct mth roots of unity are exactly the distinct nth roots of unity. □