Allman feedback.

Homework #4

Dummit and Foote Chapter 13 Selected Exercises

§13.5 #2 Find all irreducible polynomials of degree 1, 2, and 4 over $\mathbb{F}_2$ and prove that their product is $x^{16} - x$.

Solution: The only irreducible polynomials of degree 1 over $\mathbb{F}_2$ are the two linear polynomials x and $x+1$. Note that $x^2+1 = x^2-1$ in $\mathbb{F}_2[x]$, and is therefore reducible. Clearly, x^2 is reducible, leaving x^2+x+1 as the only possible irreducible polynomial. By checking $x=0$ and $x=1$, we see that x^2+x+1 has no roots in $\mathbb{F}_2$, and as it has degree less than or equal to 3, this means that x^2+x+1 is irreducible.

Let us consider polynomials of degree 4. If $f(x)$ is a polynomial in $\mathbb{F}_2[x]$ with an even number of terms, then $x=1$ is a root, and $f(x)$ is reducible. If $f(x)$ is a reducible polynomial of degree 4 with no roots over $\mathbb{F}_2$, then f must be the product of two irreducible quadratic polynomials. However, there is only one irreducible quadratic, so the only reducible polynomial of degree 4 with no roots is $(x^2+x+1)^2 = x^4+x^2+1$. Thus, the irreducible polynomials of degree 4 over $\mathbb{F}_2$ are x^4+x^3+1, x^4+x+1, and $x^4+x^3+x^2+x+1$.

Finally, we multiply all these polynomials together, to see that

$$\begin{aligned}
f(x) &= (x)(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)\\
&= (x^4+x)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)\\
&= (x^8+x^4+x^2+x)(x^8+x^4+x^2+x+1)\\
&= x^{16}+x\\
&= x^{16}-x
\end{aligned}$$

§13.5 #3 Prove that d divides n if and only if x^d-1 divides x^n-1. [Note that if $n=qd+r$ then $x^n-1 = (x^{qd+r}-x^r)+(x^r-1)$.]

Proof. First, suppose $d \mid n$. Then $n = qd$ for some $q \in \mathbb{Z}$. By dividing $x^{qd}-1$ by x^d-1 using polynomial long division, we see that

$$x^{qd}-1 = (x^d-1)(x^{qd-d}+x^{qd-2d}+\cdots+x^d+1),$$

and as $x^{qd-d}+x^{qd-2d}+\cdots+x^d+1$ is a polynomial with each monomial having coefficient 1, we have that x^d-1 divides x^n-1.

typo

d n

Next, suppose $x^n - 1$ divides $x^d - 1$. We know that by the division algorithm, there exist $r, q \in \mathbb{Z}^{\geq 0}$ such that $n = qd + r$ with either $r = 0$ or $r < d$. Then

Good.

$$\begin{aligned} x^n - 1 &= (x^{qd+r} - x^r) + (x^r - 1) \\ &= x^r(x^{qd} - 1) + (x^r - 1) \\ &= x^r(x^d - 1)(x^{qd-d} + x^{qd-2d} + \cdots + x^d + 1) + (x^r - 1). \end{aligned}$$

Because a polynomial ring is a UFD, and $x^d - 1$ divides $x^n - 1$ and $x^r(x^d - 1)(x^{qd-d} + x^{qd-2d} + \cdots + x^d + 1)$, we must have that $x^d - 1$ divides $x^r - 1$. However, this is impossible for $r \neq 0$, as $r < d$. Thus, $r = 0$ and $d \mid n$. □

§13.5 #4 Let $a > 1$ be an integer. Prove for any positive integers n, d that d divides n if and only if $a^d - 1$ divides $a^n - 1$ (cf. the previous exercise). Conclude in particular that $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ if and only if d divides n.

Proof. First, suppose that $d \mid n$. Then by the previous problem, $x^d - 1 \mid x^n - 1$. Letting $x = a$ gives us the immediate result that $a^d - 1 \mid a^n - 1$.

On the other hand, suppose $a^d - 1 \mid a^n - 1$. Then by the division algorithm, there exist $r, q \in \mathbb{Z}^{\geq 0}$ such that $n = qd + r$, where $r = 0$ or $r < d$. Then as in the previous exercise,

$$a^n - 1 = a^r(a^d - 1)(a^{qd-d} + a^{qd-2d} + \cdots + a^d + 1) + (a^r - 1).$$

Observe that $a^{qd-d} + a^{qd-2d} + \cdots + a^d + 1$ is an integer. Because $\mathbb{Z}$ is a UFD and $a^d - 1$ divides $a^n - 1$ and $a^r(a^d - 1)(a^{qd-d} + a^{qd-2d} + \cdots + a^d + 1)$, we must have that $a^d - 1$ divides $a^r - 1$. However, because $r < d$ and $a > 1$, we have that $a^r < a^d$, so $a^r - 1 < a^d - 1$, and if $r \neq 0$, we cannot have that $a^d - 1$ dividing $a^r - 1$. Thus, $r = 0$ and $d \mid n$. Nice.

Note that if we view the nonzero elements of $\mathbb{F}_{p^d}$ as a multiplicative group, then as a finite multiplicative subgroup of a field, $\mathbb{F}_{p^d}^\times$ is cyclic. Moreover, it has $p^d - 1$ elements, so every element of $\mathbb{F}_{p^d}^\times$ has multiplicative order dividing $p^d - 1$.

Suppose $d \mid n$. By the result above, $p^d - 1 \mid p^n - 1$. Choose $0 \neq \alpha \in \mathbb{F}_{p^d}$. Then

$$\alpha^{p^n} - \alpha = (\alpha^{p^n - 1} - 1)\alpha = (\alpha^{q(p^d-1)} - 1)\alpha = (1^q - 1)\alpha = 0,$$

so as α is a root of $x^{p^n} - x$, $\alpha \in \mathbb{F}_{p^n}$, and as 0 is clearly in both fields, we have that $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$.

Next, suppose $d \nmid n$. Then $p^d - 1 \nmid p^n - 1$, so $p^n - 1 = q(p^d - 1) + r$, where $0 < r < p^d - 1$. Because $\mathbb{F}_{p^d}^\times$ is cyclic, there exists an element $\alpha \in \mathbb{F}_{p^d}^\times$ with multiplicative order exactly $p^d - 1$. Therefore,

$$\alpha^{p^n} - \alpha = (\alpha^{p^n - 1} - 1)\alpha = (\alpha^{q(p^d-1)+r} - 1)\alpha = (\alpha^r - 1)\alpha.$$

Because r is less than the order of α, $p^d - 1$, we have that $\alpha^r - 1 \neq 0$. As $\alpha \neq 0$ and $\overline{\mathbb{F}_p}$ is an integral domain, $\alpha^{p^n} - \alpha \neq 0$, and $\alpha \notin \mathbb{F}_{p^n}$, so $\mathbb{F}_{p^d} \not\subseteq \mathbb{F}_{p^n}$. □

Good.

§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 is p is odd. For p odd and $n = 1$ derive *Wilson's Theorem*: $(p-1)! = -1 \mod p$.

Proof. Recall that $\mathbb{F}_{p^n}$ is defined as the splitting field for the polynomial $x^{p^n} - x = (x^{p^n-1}-1)x \in \mathbb{F}_p[x]$. Thus, the $p^n - 1$ non-zero elements of $\mathbb{F}_{p^n}$ correspond to the $p^n - 1$ distinct roots of $x^{p^n-1} - 1$. Thus,

$$x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times}(x-\alpha).$$

Plugging in $x = 0$ to the above equation, we obtain the relation

$$-1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times}(-\alpha) = (-1)^{p^n-1} \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha,$$

so $\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = (-1)^{p^n}$. Therefore, the product of all the nonzero elements of a finite field of order p^n is $+1$ if $p = 2$ (since 2^n is even for any $n \neq 0$) and -1 if p is odd (as p^n is odd for any n). ✓ Nice.

Finally, we will derive Wilson's Theorem. Observe that the nonzero elements of the field $\mathbb{F}_p$ are the numbers $1, 2, 3, \ldots, p-1$, so $\prod_{\alpha \in \mathbb{F}_p^\times} \alpha = (p-1)!$. However, as p is odd, we have that $(p-1)! = -1$ in the field $\mathbb{F}_p$, i.e., $(p-1)! \equiv -1 \mod p$. ✓ □

§13.6 #1 Suppose m and n are relatively prime positive integers. Let ζ_m be a primitive m^{th} root of unity and let ζ_n be a primitive n^{th} root of unity. Prove that $\zeta_m\zeta_n$ is a primitive mn^{th} root of unity.

Proof. First, $(\zeta_m\zeta_n)^{mn} = \zeta_m^{mn}\zeta_n^{mn} = 1^n 1^m = 1$, so $\zeta_m\zeta_n$ is a mn^{th} root of unity. ✓

In the cyclic group μ_{mn}, the element ζ_m has order m and the element ζ_n has order n. Because m and n are relatively prime, the element $\zeta_m\zeta_n$ has order mn, and thus generates μ_{mn}. Therefore, $\zeta_m\zeta_n$ is a primitive mn^{th} root of unity. □ ✓

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

Proof. Note that $(\gamma_n^d)^{\frac{n}{d}} = \gamma_n^n = 1$ so γ_n^d is a $\frac{n}{d}$ root of unity. ✓ Suppose then that there is a $0 < k < \frac{n}{d}$ such that $(\gamma_n^d)^k = 1$. Then $n|dk$ but $dk < n$ and thus γ_n^d is a primite $\frac{n}{d}$-th root of unity. ✓ □ Good.

13.6.3 Prove that if a field contains the n^{th} roots of unity for n odd then it also contains the $2n^{\text{th}}$ roots of unity.

Proof. Suppose F is a field contains the n^{th} roots of unity for n odd and suppose γ_{2n} is a $2n$-th root of unity. Note that $\gamma_{2n}^{2n} = 1$ so $\gamma_{2n}^{2n} - 1 = (\gamma_{2n}^{n})^2 - 1 = 0$ and γ_{2n}^{n} is a root of $x^2 - 1$. Since the roots of $x^2 - 1$ are ± 1 we see that either $\gamma_{2n}^{n} = 1$ and $\gamma_{2n} \in F$ or $\gamma_{2n}^{n} = -1$. In the case where $\gamma_{2n}^{n} = -1$ then $1 = \gamma_{2n}^{2n} = \gamma_{2n}^{n}\gamma_{2n}^{n} = (-1)^n\gamma_{2n}^{n} = (-\gamma_{2n})^n$ so $-\gamma_{2n} \in F$ and since F is a field, $\gamma_{2n} \in F$ as well. Thus if a field contains the n^{th} roots of unity for n odd then it also contains the $2n^{\text{th}}$ roots of unity. □

Good.

13.6.5 Prove there are only a finite number of roots of unity in any finite extension K of $\mathbb{Q}$.

Proof. Suppose K is a finite extension of $\mathbb{Q}$ with degree d and assume for contradiction that K contains infinitely many roots of unity. Let S be the set of all $m \in \mathbb{Z}$ such that K contains a primitive m^{th} root of unity. Note that S must be infinite since for each m there are only finitely many m^{th} roots of unity (and every nonprimitive k^{th} root of unity is a primitive root of unity for some $l|k$). Let $n \in \mathbb{Z}$ such that $\phi(n) > d$ and note that since S is infinite, we may choose an $m \in S$ such that $m > n$. But then K contains the field extension L generated by a primitive m^{th} root which has degree $\phi(m)$ and this implies that the order of K is greater than $\phi(m)$ which is greater than d and we see a contradiction since the order of K was d. Thus there are only a finite number of roots of unity in any finite extension K of $\mathbb{Q}$. □

degree

$[K : \mathbb{Q}]$

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

Be careful with wording. 13.6.1 says $\gamma_n\gamma_m$ is a primitive mn-th root of unity, but it does not tell you which one. Try "$\gamma_n\gamma_m = \gamma_{mn}$ where γ_{mn} is a primitive mn-th root of unity."

Proof. By 13.6.1, if $(n, m) = 1$ then $\gamma_n\gamma_n = \gamma_{nm}$. Then note that since n is odd, $(2, n) = 1$ and $\gamma_2\gamma_n = \gamma_{2n}$. But $\gamma_2 = -1$ so $\gamma_2\gamma_n = -\gamma_n$. But then $\boxed{\gamma_{2n} = -\gamma_n}$. Noting that $-\gamma_n$ is a root of $\Phi_n(-x)$, we see that $\Phi_{2n}(x)$ and $\Phi_n(-x)$ share their roots (since every root of $\Phi_{2n}(x)$ is a 2n-th root of unity) and thus $\Phi_{2n}(x) = \Phi_n(-x)$. □

13.6.10 Let ψ denote the Frobenius map $x \mapsto x^p$ on the finite field $\mathbb{F}_{p^n}$. Prove that ψ gives an isomorphism of $\mathbb{F}_{p^n}$ to itself (such an isomorphism is called an automorphism). Prove that ψ^n is the identity map and no lower power of ψ is the identity.

Proof. Let $a, b \in \mathbb{F}_{p^n}$ and note that $\psi(a+b) = (a+b)^p = a^p + b^p = \psi(a) + \psi(b)$ since $\mathbb{F}_{p^n}$ has characteristic p. Further, $\psi(ab) = (ab)^p = a^pb^p = \psi(a)\psi(b)$ so we see that ψ is a ring homomorphism. Suppose for some x that $\psi(x) = 0$. Then $0 = x^p$ and since $\mathbb{F}_{p^n}$ is a field, there are no zero divisors and $x = 0$. From this we see that the kernal is trivial and thus that this homomorphism is $1-1$. Further, since $\mathbb{F}_{p^n}$ is finite it follows that if ψ is 1-1 then ψ is also onto and we note that ψ is a bijection and thus an isomorphism from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$. I.e., ψ is an automorphism.

Let $x \in \mathbb{F}_{p^n}^{\times}$ and note that $x^{p^n} = x$ (ref 13.5.6). It follows that $\psi^n(x) = (x^p)^n = x^{pn} = x$ so ψ^n is the identity map.

Suppose for contradition that there is a $0 < k < n$ such that ψ^k is the identity. Then $\psi^k(x) = (x^p)^k = x^{pk} = x$ so $x^{pk} - x = 0$ and every element of $\mathbb{F}_{p^n}$ is a root of $x^{pk} - x$ so by 13.5.3 we see that $n|k$ so $n \leq k$ and n is the smallest integer such that ψ^n is the identity map. $\square$

too many roots.