Q1 Problem 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 $a^n - 1$.

Proof. If d divides n, i.e. $n = dq$ for some positive integer q, then

$$a^n - 1 = a^{dq} - 1 = (a^d - 1)\left((a^d)^{q-1} + (a^d)^{q-2} + \cdots + a^d + 1\right).$$

Evidently, $a^d - 1$ divides $a^n - 1$.

Now assume $a^d - 1$ divides $a^n - 1$. Since $a > 1$ and n, d are positive, then $a^d \leq a^n$ implies $d \leq n$. Euclidean division gives us $n = dq + r$ for some nonnegative integers q, r, with $r < d$. We write

$$\begin{aligned} a^n - 1 &= a^{dq+r} - 1 \\ &= (a^{dq+r} - a^r) + (a^r - 1) \\ &= a^r(a^{dq} - 1) + (a^r - 1) \\ &= a^r(a^d - 1)\left((a^d)^{q-1} + (a^d)^{q-2} + \cdots a^d + 1\right) + (a^r - 1). \end{aligned}$$

Therefore, $a^d - 1$ divides

$$(a^n - 1) - a^r(a^d - 1)\left((a^d)^{q-1} + (a^d)^{q-2} + \cdots a^d + 1\right) = a^r - 1,$$

implying that either $a^d - 1 \leq a^r - 1$ or $a^r - 1 = 0$. The former cannot be true, as it would imply $d \leq r$, but we know $r < d$. Therefore, we must have $a^r - 1 = 0$, so $r = 0$. Hence, $n = dq$, meaning d divides n.

□

Conclude in particular that $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ if and only if d divides n.

Proof. If $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$, then $\mathbb{F}_{p^d}^\times$ is a subgroup of $\mathbb{F}_{p^n}^\times$ under multiplication. By Lagrange's theorem, $|\mathbb{F}_{p^d}^\times| = p^d - 1$ divides $|\mathbb{F}_{p^n}^\times| = p^n - 1$, and the previous result implies d divides n.

If d divides n, then $p^d - 1$ divides $p^n - 1$, by the previous result. Moreover, it is essentially the same proof to show $x^{p^d-1} - 1$ divides $x^{p^n-1} - 1$ in any polynomial field. We deduce that $x^{p^d} - x$ divides $x^{p^n} - x$, telling us that $x^{p^d} - x$ splits completely in $\mathbb{F}_{p^n}$, the splitting field for $x^{p^n} - x$. Since $\mathbb{F}_{p^d}$ is the unique splitting field of $x^{p^d} - x$ contained in $\overline{\mathbb{F}_p}$, then we must, therefore, have $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$.

□

Q2 Problem 13.5.6 Prove that $x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (x - \alpha)$.

Proof. We have seen that $\mathbb{F}_{p^n} \subseteq \overline{\mathbb{F}_p}$ is precisely the set of p^n distinct roots of

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

in $\overline{\mathbb{F}_p}$. So $\mathbb{F}_{p^n}^\times$ is a set of $p^n - 1$ distinct roots of $x^{p^n-1} - 1$ in $\overline{\mathbb{F}_p}$. Since $x^{p^n-1} - 1$ has at most $p^n - 1$ roots in $\overline{\mathbb{F}_p}$, counting multiplicity, and we know of at least $p^n - 1$ distinct roots, then all roots must be simple. Since $\mathbb{F}_{p^n}^\times$ is precisely the set of $p^n - 1$ distinct simple roots, then $x^{p^n-1} - 1$ is separable with decomposition

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

□

Conclude that $\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = (-1)^{p^n}$ so the product of nonzero elements of finite fields is $+1$ if $p = 2$ and -1 if p is odd.

We evaluate the previous result at $x = 0$.

$$\begin{aligned} 0^{p^n-1} - 1 &= \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (0 - \alpha) \\ -1 &= \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (-1)\alpha \\ -1 &= (-1)^{p^n-1} \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha \\ (-1)^{p^n} &= (-1)^{2(p^n-1)} \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha \\ (-1)^{p^n} &= \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha \end{aligned}$$

This value of the left-hand side is $+1$ if $p = 2$, and -1 if p is odd.

For p odd and $n = 1$ derive *Wilson's theorem*: $(p-1)! \equiv -1 \pmod{p}$.

In this case, the above result is $\prod_{\alpha \in \mathbb{F}_p} \alpha = -1$. Since the elements of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ are the integers $0, 1, \ldots, p-1$, then $(p-1)! = \prod_{\alpha \in \mathbb{F}_p} \alpha = -1$ in $\mathbb{F}_p$. And equality in $\mathbb{F}_p$ is precisely equivalence of integers modulo p, so this means $(p-1)! \equiv -1 \pmod{p}$.

Q3 Let F be a field and K be a splitting field of $f(x) \in F[x]$. Show that if $f(x)$ is separable then K/F is separable.

Proof. Since $f(x)$ splits completely in $K[x]$, then $f(x) = a(x - \alpha_1) \cdots (x - \alpha_n)$ for some $a \in F^\times$ and $\alpha_1, \dots, \alpha_n \in K$. Let $S = \{\alpha_1, \dots, \alpha_n\}$ be the set of roots of $f(x)$ (ignoring multiplicity, i.e., not a multiset), then $f(x)$ splits completely over $F(S) \subseteq K$. And since K is a splitting field for $f(x)$, then in fact $F(S) = K$. For each $\alpha \in S$, $f(\alpha) = 0$, so its minimal polynomial $m_{\alpha,F}(x) \in F[x]$ divides $f(x)$. Since $f(x)$ is separable, then $m_{\alpha,F}(x)$ must also be separable, otherwise $m_{\alpha,F}(x)$ would have some multiple roots. Therefore, α is separable over F, implying every element of S is separable over F. And since $K = F(S)$, we conclude that K/F is separable.

$\square$

Q4 Show that $\mathbb{F}_2[x]/(x^3+x+1) \cong \mathbb{F}_2[y]/(y^3+y^2+1)$ and find an explicit isomorphism.

Proof. We define a ring homomorphism

$$\begin{aligned} \varphi : \mathbb{F}_2[x] &\to \mathbb{F}_2[y] \\ p(x) &\mapsto p(y+1) \end{aligned}$$

which is the evaluation of $p(x)$ at $y+1 \in \mathbb{F}_2[y]$. We can see that φ is a ring isomorphism, with inverse given by the evaluation map $p(y) \mapsto p(x+1)$. Let $I = (x^3+x+1)$ and $J = (y^3+y^2+1)$ denote the ideals in their respective polynomial rings. Composition of φ with the natural projection

$$\begin{aligned} \pi : \mathbb{F}_2[y] &\to \mathbb{F}_2[y]/J \\ p(y) &\mapsto \overline{p(y)} \end{aligned}$$

yields a surjective ring homomorphism

$$\sigma = \pi \circ \varphi : \mathbb{F}_2[x] \to \mathbb{F}_2[y]/J.$$

From the first isomorphism theorem, we have

$$\mathbb{F}_2[x]/\ker\sigma \cong \mathbb{F}_2[y]/J.$$

It remains to prove that $\ker\sigma = I$. By definition, $\ker\sigma$ is the set of elements $p(x) \in \mathbb{F}_2[x]$ such that $\varphi(p(x)) \in \ker\pi = J$. We compute

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

For any $p(x) \in I$, there is some $q(x) \in \mathbb{F}_2[x]$ such that $p(x) = q(x)(x^3+x+1)$, so

$$\varphi(p(x)) = \varphi(q(x))\varphi(x^3+x+1) = q(y+1)(y^3+y^2+1) \in J.$$

Hence, $\varphi(I) \subseteq J$, so $I \subseteq \varphi^{-1}(J)$. And since $\varphi^{-1}(y^3+y^2+1) = x^3+x+1$, then by the same argument, $\varphi^{-1}(J) \subseteq I$. Therefore, we obtain the equality $\ker\sigma = \varphi^{-1}(J) = I$.

□

Q5 Let F be a field of characteristic p. Show that if F is perfect, then $F = F^p$.

Proof. We will prove the contrapositive. Suppose $F \neq F^p$, and let $a \in F$ such that a is not a pth power in F. Consider the polynomial $x^p - a \in F[x]$. If $\alpha \in \overline{F}$ is a root of $x^p - a$, then $\alpha \notin F$ and $\alpha^p = a$. So in $\overline{F}[x]$,

$$x^p - a = x^p - \alpha^p = (x - \alpha)^p.$$

Therefore, α is the unique root of $x^p - a$ in $\overline{F}$ (equivalent to saying the Frobenius endomorphism on $\overline{F}$ is injective). Since α is a root of $x^p - a$, then $m_{\alpha,F}(x) \bigm| (x - \alpha)^p$, so $m_{\alpha,F}(x) = (x - \alpha)^n$ for some $n \geq 1$. Since $\alpha \notin F$, then we must have $n \geq 2$, implying that α is a multiple root of $m_{\alpha,F}(x)$. In particular, $m_{\alpha,F}(x)$ is not separable, so α is algebraic but not separable over F. Therefore, $F(\alpha)/F$ is a finite field extension which is not separable, i.e., F is not perfect.

$\square$