Paul Gustafson
Texas A&M University - Math 416
Instructor: Dr. Papanikolas

HW 4, due 3/5

33.10 Show that every irreducible polynomial in $\mathbb{F}_p[x]$ is a divisor of $x^{p^n} - x$ for some n.

Proof. Let $f \in \mathbb{F}_p[x]$ be irreducible. WLOG f is non-zero. Let E be the finite extension of $\mathbb{F}_p$ given by adjoining all the roots of f. Let $n = [E : \mathbb{F}_p]$. We know from class that every element of E is a root of $g(x) := x^{p^n} - x$. Hence, every root of f is a root of g. Hence, for every root α of f, the evaluation map w.r.t. α vanishes at both f and g.

Thus, it suffices to show that f is separable (has no double roots in $\overline{\mathbb{F}}_p$). Since $\mathbb{F}_p[x]$ is a PID, there exists $h \in \mathbb{F}_p[x]$ such that $\langle h \rangle = \langle f, g \rangle \subset \mathbb{F}_p[x]$. If f has no roots over $\overline{\mathbb{F}}_p$, it is trivially separable. Otherwise, let α be a root of f, h also vanishes at α. Since h cannot be the zero polynomial, h is a nonconstant divisor of f. Since f is irreducible, we have $h = f$. Hence, f divides g. Moreover, since g is separable, so is f. □

12 Show that a finite field of p^n elements has exactly one subfield of p^m elements for each divisor m of n.

Proof. Fix m and n with $n = md$. Recall that every field of p^n elements is isomorphic to the field $K := \{x \in \overline{\mathbb{F}}_p : x^{p^n} - x = 0\}$. This isomorphism bijectively maps subfields to subfields. Note that by a theorem proved in class, $E := \{x \in \overline{\mathbb{F}}_p : x^{p^m} - x = 0\}$ is the only field of order p^m in $\overline{\mathbb{F}}_p$. Thus, if $E \subset K$, it is unique.

Let the Frobenius map $\phi : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ be defined by $\phi(x) = x^p$. Let ϕ^k for $k \in \mathbb{N}$ denote k compositions of ϕ.

Let $\alpha \in E$. Note that $\phi^m(\alpha) = \alpha$ by the definition of E. Hence, $\alpha^{p^n} = \phi^n(\alpha) = \phi^{md}(\alpha) = \phi^{m(d-1)}(\phi^m(\alpha)) = \phi^{m(d-1)}(\alpha) = \ldots = \alpha$. Thus, $\alpha \in K$, so $E \subset K$. □

13 Show that $x^{p^n} - x$ is the product of all monic irreducible polynomials in $\mathbb{F}_p[x]$ of a degree d dividing n.

Proof. Let d divide n, and f be a monic irreducible of degree d. Then the splitting field of f over $\mathbb{F}_p$—that is, $\mathbb{F}_p$ adjoined the roots of f in $\overline{\mathbb{F}}_p$—is of degree d over $\mathbb{F}_p$, so has p^d elements. By (12), this field lies within $\mathbb{F}_p^n$; hence, every root of f over $\overline{\mathbb{F}}_p$ is also a root of $x^{p^n} - x$.

Conversely, let $\alpha \in \overline{\mathbb{F}}_p$ be a root of $x^{p^n} - x$. Then $\alpha \in \mathbb{F}_{p^n}$, so since $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, the degree of the monic irreducible for α over $\mathbb{F}_p$ must divide n.

Hence, the roots of $x^{p^n} - x$ in $\overline{\mathbb{F}}_p$ are precisely the roots of the monic irreducibles of degree d dividing n. From class, we know that the roots of $x^{p^n} - x$

are distinct, so it suffices to show that if α is of degree d, where $d \mid n$, then α is a single root of precisely one monic irreducible.

But we already know that every α is a root of a unique monic irreducible, and from the proof of (10), this polynomial is separable. $\square$

14 Let p be an odd prime.
a. Show that a is a quadratic residue modulo p iff $a^{(p-1)/2} = 1(\mod p)$.
b. Is $x^2 - 6$ irreducible in $\mathbb{Z}_{17}[x]$?

Proof. For (a), first note that the set R of quadratic residues modulo p form a subgroup of $\mathbb{F}_p^\times$. Indeed, the map $x \mapsto x^2$ is an endomorphism of $\mathbb{F}_p^*$. The kernel of this map consists of the roots of the polynomial $x^2 - 1$ over $\mathbb{F}_p$, i.e. ± 1. Since $p > 2$, 1 and -1 are distinct, so R is of index 2 in $\mathbb{F}_p^*$

If $a = b^2$ for some $b \in \mathbb{F}_p^*$, then $a^{(p-1)/2} = b^{p-1} = 1$. On the other hand, the equation $x^{(p-1)/2} = 1$ has at most $(p-1)/2$ roots in $\mathbb{F}_p^*$, and we know that all $(p-1)/2$ quadratic residues are roots. Hence, if a is not a quadratic residue, $a^{(p-1)/2} \neq 1$.

For (b), note that $6^{(17-1)/2} = 6^8 = 16 \pmod{17}$. Hence, 6 is not a quadratic residue mod 17; that is, $x^2 - 6$ is irreducible in $\mathbb{Z}_{17}[x]$. $\square$

34.3 In the group $\mathbb{Z}_{24}$, let $H = \langle 4 \rangle$, and $N = \langle 6 \rangle$.
a. List the elements of HN and $H \cap N$.
b. List the cosets in HN/N, showing the elements in each coset.
c. List the cosets in $H/(H \cap N)$, showing the elements in each coset.
d. Give the correspondence between HN/N and $H/(H \cap N)$ described in the proof of Theorem 34.5.

Proof. **a.** HN: the even elements of $\mathbb{Z}_{24}$. $H \cap N = \{0, 12\}$.
b. HN/N: $\{N, 2+N, 4+N\}$. $N = \{0, 6, 12, 18\}$. $2 + N = \{2, 8, 14, 20\}$. $4 + N = \{4, 10, 16, 22\}$.
c. $H/(H \cap N)$: $\{\{0, 12\}, \{4, 16\}, \{8, 20\}\}$.
d. $N \mapsto \{0, 12\}$; $2 + N \mapsto \{4, 16\}$; $4 + N \mapsto \{8, 20\}$. $\square$

8 Let $H < K < L < G$ with H, K, L normal in G. Let $A = G/H$, $B = K/H$, and $C = L/H$.
a. Show that B and C are normal subgroups of A, and $B < C$.
b. To what factor group of G is $(A/B)/(C/B)$ isomorphic?

Proof. **a.** Suppose $kH \in B$ and $gH \in A$. Since H, K are normal in G, we have $gH(kH)(gH)^{-1} = gkg^{-1}H = kH$. Thus, B is normal in A. A similar argument shows C is normal in A.

Lastly, if $b \in B$, then for some $k \in K \subset L$, we have $k \in b$. Hence, $b = kH \in L/H = C$.
b. By Theorem 34.7, $(A/B)/(C/B) \simeq A/C$. By the same theorem, $A/C \simeq G/K$. $\square$