Math 340 Tutorial
November 24th

Question 1. Let K be a finite degree extension of a finite field F. Show there exists and element $a \in K$ for which $K = F(a)$.

Question 2. How many primitive elements of $GF(81)$ are there? Of GF(32)?

Question 3. Determine the finite fields whose largest proper subfield is GF(2^5).

Question 4. Let $\alpha, \beta \in$ GF(81) with $|\alpha| = 5$ and $|\beta| = 16$. Show that $\alpha\beta$ is a primitive element.

Question 5. Let p be an odd prime, and let $a \in$ GF(p) be a nonsquare. Show that a is a square in GF(p^n) if n is even, and a is a nonsquare in GF(p^n) if n is odd.

Define $f \in F[x]$ by $f(x) = x^n - 1$. The roots of f are the n-roots of unity over F, and the splitting field $F^{(n)}$ of f over F is the n-th cyclotomic field (over F). Use $E^{(n)}$ to denote the roots of f.

Question 6. Suppose that char(F) $= p$, a prime. Show: **(a)** If $(p, n) = 1$, then $E^{(n)}$ is a multiplicative cyclic group of order n. **(b)** If $p \mid n$, write $n = mp^e$ with $(p, m) = 1$. Then $F^{(m)} = F^{(n)}$ and $E^{(m)} = E^{(n)}$, and the roots of f in $F^{(n)}$ are the elements of $E^{(m)}$ each with multiplicity p^e.

Suppose that $(p, n) = 1$, and let ζ be a generator of $E^{(n)}$. The polynomial

$$Q_n(x) = \prod_{\substack{s=1 \\ (s,n)=1}}^{n} (x - \zeta^s)$$

is called the n-th cyclotomic polynomial over F.

Question 7. Show:

(a) $x^n - 1 = \prod_{d|n} Q_d(x)$.

(b) $Q_n(x) = \prod_{d|n} (x-1)^{\mu(n/d)}$.

(c) $Q_{p^k}(x) = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \cdots + x^{(p-1)p^{k-1}}$.

(d) If $F =$ GF(q) with $(q, n) = 1$, then Q_n factors into $\phi(n)/d$ distinct monic irreducible polynomials in $F[x]$ of the same degree d, $F^{(n)}$ is the splitting field of any such factor over F, and $[F^{(n)} : F] = d$, where d is multiplicative order of q modulo n.

Question 8. Let $f \in$ GF(q)$[x]$ have degree m with $f(0) \neq 0$. Show there exists a positive integer $e \leqq q^m - 1$ such that f divides $x^e - 1$.

For a polynomial $f \in$ GF(q)$[x]$ with $f(0) \neq 0$, the order ord(f) of f is the smallest positive integer e for which $f \mid x^e - 1$. If $x \mid f$, write $f = x^a g$ with $g(0) \neq 0$. We then define ord(f) $\equiv$ ord(g).

Question 9. Let $f \in$ GF(q)$[x]$ be irreducible of degree m with $f(0) \neq 0$. Show that ord(f) is the multiplicative order of any one of its roots in GF(q^m). Show additionally that ord(f) $\mid q^m - 1$.

Question 10. Show the number of monic irreducible polynomials in GF(q)$[x]$ of degree m and order e is $\phi(e)/m$ if $e \geqq 2$ and m is the multiplicative order of q modulo e, equal to 2 if $m = e = 1$, and equal

to 0 in all other cases.

Question 11. Show that $f \in \mathrm{GF}(q)[x]$ is an irreducible factor of $x^{q^n} - x$ if and only if $\deg(f) \mid n$. Moreover, show that the product of all irreducible polynomials whose degree divides n is equal to $x^{q^n} - x$.

Question 12. Let $N_q(n)$ be the number of irreducible polynomials over $\mathrm{GF}(q)$ of degree n. Show that

$$N_q(n) = \sum_{d|n} \mu(n) q^{n/d}.$$

Question 13. Let $I(q, n, x)$ be the product of all irreducible polynomials in $\mathrm{GF}(q)[x]$ of degree n. Show that

$$I(q, n, x) = \prod_{d|n} (x^{q^d} - x)^{\mu(n/d)} = \prod Q_m(x)$$

where the product is extended over all divisor m of $q^n - 1$ such that n is multiplicative order of q modulo m.