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 $K = F(a)$.

We know that there exists some $\alpha \in K^*$ for which $K^* = \langle \alpha \rangle$. But then $K = F(\alpha)$.

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

We have the number of primitive elements of GF(81) is $\phi(80) = \phi(2^4 5) = 2^3 4 = 32$. The number of primitive elements of GF(32) is $\phi(31) = 30$.

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

GF(2^{10}).

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

Since $(5, 16) = 1$, we have $\langle \alpha \rangle \times \langle \beta \rangle = \{1\}$ and hence $|\langle \alpha\beta \rangle| = 5 \cdot 16 = 80$.

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.

Let g be a primitive element of GF(p^n), and let $v = \frac{q^n-1}{q-1} = q^{n-1} + q^{n-2} + \cdots + q + 1$. Then g^v is a primitive element of GF(p). Since $a \in$ GF(p), $a \neq 0$, we have there is some $k \in \{1, 3, \ldots, p-2\}$ for which $a = g^{vk}$; in particular, k is odd by our assumption on a. The parity of v equals the parity of n. Hence, vk is even if and only if n is even.

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.

(a) We have $E^{(n)} \neq \emptyset$ as $1 \in E^{(n)}$. If $a, b \in E^{(n)}$, then $(ab^{-1})^n = a^n(b^n)^{-1} = 1 \cdot 1 = 1$; hence, $ab^{-1} \in E^{(n)}$.

(b) This is clear because $x^n - 1 = x^{mp^e} - 1 = (x^m - 1)^{p^e}$; so, the result follows from part (a).

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 $F = \mathrm{GF}(q)$ 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.

(a) Each n-th root of unity is a primitive d-th root of unity for exactly one divisor d of n. Explicitly, if ζ is a primitive n-th root of unity, and if ζ^s is an arbitrary n-root of unity, then $d = n/(s,n)$. Since

$$Q_n(x) = \prod_{s=0}^{n-1}(x-\zeta^s),$$

the result follows by collecting those factors $x - \zeta^s$ which are primitive d-th roots of unity.

(b) Apply the multiplicative version of Möbius inversion to part (a).

(c) By induction on k. If $k = 1$, the result is clear. Assume it is true for $k \geqq 1$. Then $Q_{r^{k+1}} = \frac{x^{r^{k+1}}-1}{\prod_{s=0}^{k} Q_{r^s}(x)} = \frac{x^{r^{k+1}}-1}{x^{r^k}-1}$.

(d) If ζ is a primitive n-th root of unity, then $F^{(n)}$ is the algebraic extension $F(\zeta)$. Observe that $\zeta \in \mathrm{GF}(q^k)$ if and only if $\zeta^{q^{k-1}} - 1 = 0$ if nad only if $q^k \equiv 1 \pmod{n}$. The smallest k for which this holds is $k = d$. So, $\zeta \in \mathrm{GF}(q^d)$ but no proper subfield thereof. Thus, the minimal polynomial of ζ has degree d, and since ζ was an arbitrary root of $Q_n(x)$, the result follows.

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

The ring $\mathrm{GF}(q)[x]/(f)$ has order q^m. Therefore, among the residues $x^k + (f)$, $k = 0, \ldots, q^m - 1$, there must be $a < b$ for which $x^a \equiv x^b \pmod{f}$. Since $(x, f) = 1$, we have that $x^{a-b} \equiv 1 \pmod{f}$. Therefore, $f \mid x^{a-b} - 1$ and $0 < a - b \leqq q^m - 1$.

For a polynomial $f \in \mathrm{GF}(q)[x]$ with $f(0) \neq 0$, the order $\mathrm{ord}(f)$ 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 $\mathrm{ord}(f) \equiv \mathrm{ord}(g)$.

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

$\mathrm{GF}(q^m)$ is the splitting field of f. The roots of f have the same order in $\mathrm{GF}(q^m)^*$. But $\alpha^e = 1$ if and only if $f \mid x^e - 1$. The result now follows.

Question 10. Show the number of monic irreducible polynomials in $\mathrm{GF}(q)[x]$ 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.

Let $f \in \mathrm{GF}(q)[x]$ be irreducible with $f(0) \neq 0$. Then $\mathrm{ord}(f) = e$ if and only if every root of f is a primitive e-th root of unity over $\mathrm{GF}(q)$ if and only if $f \mid Q_e(x)$. We've shown every monic irreducible factor of $Q_e(x)$ has the same degree m, the least positive integer such that $q^m \equiv 1 \pmod{e}$. The number of such factors must then be $\phi(e)/m$. For $m = e = 1$ we also have to take into account $f(x) = x$.

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 $x^{q^n} - x$.

Let f be an irreducible divisor of $x^{q^n} - x$, and let α be a root of f. Then $\alpha \in \mathrm{GF}(q^n)$ whence $\mathrm{GF}(q)(\alpha)$ is a subfield of $\mathrm{GF}(q^n)$. But then $[\mathrm{GF}(q)(\alpha) : \mathrm{GF}(q)] = m$ divides $[\mathrm{GF}(q^n) : \mathrm{GF}(q)] = n$.

Conversely, if m divides n, then $\mathrm{GF}(q^m) \subseteqq \mathrm{GF}(q^n)$. Furthermore, if α is a root of f, then $\mathrm{GF}(q)(\alpha) = \mathrm{GF}(q^m)$; hence, $\alpha \in \mathrm{GF}(q^n)$ and so $f \mid x^{q^n} - x$.

We have shown that the monic irreducible factors f of $x^{q^n} - x$ are exactly those whose degrees divide n. We know $x^{q^n} - x$ has no repeated roots, so every irreducible factor of $x^{q^n} - x$ appears exactly once.

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

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

The previous question implies $q^n = \sum_{d \mid n} d N_d(q)$. The result now follows from Möbius inversion.

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

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

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

We've observed already that $x^{q^n} - x = \prod_{d \mid n} I(q, d, x)$; so, the first identity follows from Möbius inversion. Next, let $S \subseteqq \mathrm{GF}(q^n)$ be the set of elements of degree n. Thus each $\alpha \in S$ is a root of $I(q, n, x)$. On the other hand, if β is a root of $I(q, n, x)$, then β is a root of some monic irreducible of degree n, hence $\beta \in S$. We therefore have

$$I(q, n, x) = \prod_{\alpha \in S} (x - \alpha).$$

Now $\mathrm{ord}(\alpha) = m$, $\alpha \in S$, is such that $n = \mathrm{ord}_m(q)$. For such a divisor m of $q^n - 1$, let $S_m \subseteqq S$ be the subset of elements of S of order m. Then S is the disjoint union of the S_m, hence

$$I(q, n, x) = \prod_m \prod_{\alpha \in S_m} (x - \alpha).$$

Now S_m contains all the elements of $\mathrm{GF}(q^n)^*$ of order m, i.e., all the primitive m-th roots of unity over $\mathrm{GF}(q)$. It follows that

$$\prod_{\alpha \in S_m} (x - \alpha) = Q_m(x).$$