Ninth Homework Assignment

Turn-in problems due 11/19? (10 pts. apiece): Chapter 22 Any even problem....

2: Suppose $m|n$. Then $GF(p^m)$ is a subfield of $GF(p^n)$ by Theorem 22.3. By the multiplication theorem for towers of fields, we have $n = [GF(p^n) : GF(p)] = [GF(p^m) : GF(p^m)][GF(p^n) : GF(p)] = [GF(p^m) : GF(p^m)]m$, implying that $[GF(p^n) : GF(p^m)] = n/m$ as required.

4: Since $GF(81)^*$ is a cyclic group, it is isomorphic to $\mathbb{Z}_{16} \oplus \mathbb{Z}_5$. The number of generators of this abelian group is $8 \times 4 = 32$ (since there are 8 generators of $\mathbb{Z}_{16}$ and 4 generators of $\mathbb{Z}_5$).

6: Both of the polynomials are irreducible over $GF(3)$ and hence both of the factor rings are isomorphic to $GF(9)$.

8: The possible finite fields whose largest proper subfield is $GF(2^5)$ is $GF(2^{5p})$ for $p$ a prime at most 5 (this is true by applying Theorem 22.3). Thus, the fields are $GF(2^{10}), GF(2^{15})$, and $GF(2^{25})$.

10: The smallest field with exactly 6 subfields is $GF(2^{12})$ (there is precisely one subfield for each divisor of the exponent on 2, and 12 is the smallest positive integer with precisely 6 divisors, namely 1,2,3,4,6, and 12).

12: Every nonzero, non-unity element of the factor ring will be a generator of the cyclic multiplicative group since the multiplicative group has order 31 which is prime. A corollary of Lagrange's theorem in group theory implies that the order of an element must divide the order of the group and hence every nonidentity element in the multiplicative group of the field has order 31 and is a generator of the group.

14: The factor ring is a field with 27 elements and hence the multiplicative group is cyclic of order 26. Every nonidentity element in the multiplicative group has order 2, 13, or 26. The element $x$ cannot have order 2 (if it does, then $x = \pm 1$ in the factor group, but that is not the case), so $x$ either has order 13 or 26. If it has order 26, then we are done since $x$ would be a generator of the multiplicative group of the field. Suppose $x$ has order 13: then $(2x)^{13} = ((-1)x)^{13} = (-1)^{13}x^{13} = -1$. Since $2x$ also cannot have order 2 (same reasoning) and it doesn’t have order 13, it must have order 26 and hence is a generator.
16: The order of $\alpha \beta$ is the least common multiple of the orders of $\alpha$ and $\beta$ because multiplication in the field is commutative. Thus, the order is 80 and $\alpha \beta$ is a generator as claimed.

18: Subgroups of cyclic groups are cyclic, and the multiplicative group of a field is cyclic.

20: Suppose $g(x)$ is irreducible over $GF(p)$ and $g(x)|(x^{p^n} - x)$. Then $GF(p)[x]/\langle g(x) \rangle$ is isomorphic to $GF(p^k)$ for $k = \deg(g(x))$. Since $g(x)|(x^{p^n} - x)$, we must have that $GF(p^k)$ is a subfield of $GF(p^n)$, and hence $k|n$.

22: Since 18 has precisely 6 divisors (including 1 and 18), there are 6 subfields in the lattice, and since 30 has precisely 8 divisors (including 1 and 30), there are 8 subfields in the second lattice.

24: Suppose $p(x)$ is a polynomial in $\mathbb{Z}_p[x]$ with no multiple zeros. We can write $p(x)$ as a product of irreducibles and do the tower of field extensions found by modding out by one irreducible at a time. The top of this tower will be the splitting field for $p(x)$, and every element in that top field will be a zero of $x^{p^n} - x$. Since all of the zeros of $p(x)$ are in this field (and there are no multiple zeros), we must have that $p(x)$ divides $x^{p^n} - x$.

26: This problem is imprecisely stated! The splitting field of a cubic irreducible polynomial will be $GF(p^3)$, formed by modding out the polynomial ring with coefficients in $\mathbb{Z}_p$ by the ideal generated by the cubic irreducible polynomial. If $\alpha$ is a root of the cubic irreducible polynomial in the extension, then $\alpha^p$ and $\alpha^{p^2}$ are also roots in that extension and the polynomial splits. Freshmen exponentiation strikes again!

28: There are two proper subfields. If $\alpha$ is a generator of the cyclic multiplicative group of $GF(2^{10})$, then $\langle \alpha^{33} \rangle \cup \{0\} = GF(32)$ and $\langle \alpha^{341} \rangle \cup \{0\}$ are the two proper subfields.

30: We didn’t talk about algebraically closed, but we could note here that $GF(p^{2n})$ is an extension of $GF(p^n)$ that is finite dimensional and hence algebraic, so there are elements of the bigger field that are roots of polynomials with coefficients in the smaller field, and the polynomials are not just linear.

32: The intersection will have $p^{gcd(s,t)}$ elements.

* problem, 40 pts.: Let $E = GF(p^n)$ for $p$ a prime and $n$ a positive integer. Define the Trace function $Tr : GF(p^n) \to GF(p)$ by $Tr(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}}$ for all $\alpha \in GF(p^n)$.

a.: Show that $Tr(\alpha) \in GF(p)$ for all $\alpha \in GF(p^n)$. (Hint: show that $Tr(\alpha)$ is a coefficient for the minimum polynomial for $\alpha$ over $GF(p)$.)
Suppose \( f(x) \) is the minimum polynomial for \( \alpha \) over \( GF(p) \): by Freshmen exponentiation (or more traditionally the Frobenius automorphism), \( \alpha^p, 1 \leq i \leq n \) are all of the roots of \( f(x) \) (some might be repeated). We observe that the maximum possible degree for \( f(x) \) is \( n \): if the degree of \( f \) is bigger than \( n \), then \( \alpha \) would have to be in a bigger extension than \( GF(p^n) \). To show that \( f(x) \) splits in \( GF(p^n) \), we first observe that \( \phi : GF(p^n) \rightarrow GF(p^n) \) defined by \( \phi(\beta) = \beta^p \) is an automorphism (we have shown this many times this semester). This automorphism can be extended to an automorphism of \( GF(p^n)[x] \) by \( \phi(a_m x^m + \cdots + a_1 x + a_0) = \phi(a_m) x^m + \cdots + \phi(a_1) x + \phi(a_0) \) for \( a_i \in GF(p^n) \). Since \( \alpha \) is a root of \( f(x) \) in \( GF(p^n) \), we have that there is a \( g(x) \in GF(p^n)[x] \) so that \( f(x) = (x - \alpha) g(x) \). Applying \( \phi \) to this polynomial equation yields \( f(x) = \phi(f(x)) = \phi((x - \alpha) g(x)) = (x - \phi(\alpha)) \phi(g(x)) = (x - \alpha^p) \phi(g(x)) \). Thus, \( \alpha^p \) is also a root of \( f(x) \), and we can keep applying \( \phi \) to get all of the \( p^k \) powers of \( \alpha \) as roots of \( f(x) \). If there were more roots of \( f(x) \) than the \( p^k \) powers of \( \alpha \), then the degree of \( f(x) \) would be more than \( n \) and the extension \( GF(p)[x]/\langle f(x) \rangle \) would be bigger than \( p^n \). We can now write \( f(x) = (x - \alpha)(x - \alpha^p) \cdots (x - \alpha^{p^n}) \) for some \( k \mid n \). The coefficient on the \( x^{k-1} \) term is \(-\alpha - \alpha^{p^2} - \cdots - \alpha^{p^k}\), and it is in \( GF(p) \) since all of the coefficients of \( f \) are in \( GF(p) \).

If \( k < n \), then \( Tr(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^k} + \alpha^{p^k+1} + \cdots + \alpha^{p^n} = \alpha + \alpha^p + \cdots + \alpha^{p^k} + \alpha + \cdots + \alpha^p = 2(\alpha + \alpha^p + \cdots + \alpha^p) \). Since \(-\alpha + \alpha^p + \cdots + \alpha^p) \in GF(p) \), we have that \( Tr(\alpha) \in GF(p) \) as claimed.

b.: Show that \( Tr \) is a linear transformation. (Take any linear combination of elements from \( E \) and show that the linear transformation properties hold for that combination.)

Let \( \beta, \gamma \in E, a, b \in GF(p) \). We compute the following:
\[
\begin{align*}
Tr(a\beta + b\gamma) &= (a\beta + b\gamma) + (a\beta + b\gamma)p + (a\beta + b\gamma)p^2 + \cdots + (a\beta + b\gamma)p^n \\
&= (a\beta + b\gamma) + (a\beta^p + b\gamma p) + (a\beta^p + b\gamma^p) + \cdots + (a\beta^p + b\gamma^p) + (a\beta^p + b\gamma^p) + \cdots + (a\beta^{p^n} + b\gamma^{p^n}) + (a\beta + b\gamma) + (a\beta^{p^2} + b\gamma^{p^2}) + \cdots + (a\beta^{p^n} + b\gamma^{p^n}) = a Tr(\beta) + b Tr(\gamma).
\end{align*}
\]
I used the fact that \( \phi^p = c \) for every \( c \in GF(p) \).

c.: For a given \( \beta \in GF(p^n) \), show that the map \( \phi_{\beta} \) defined to be \( \phi_{\beta}(\alpha) = Tr(\beta\alpha) \) is a linear transformation.

Let \( \eta, \zeta \in E, a, b \in GF(p) \). We compute the following:
\[
\begin{align*}
\phi_{\beta}(a\eta + b\zeta) &= Tr(\beta(a\eta + b\zeta)) = Tr(a(\beta\eta) + b(\beta\zeta)) = a Tr(\beta\eta) + b Tr(\beta\zeta) = a \phi_{\beta}(\eta) + b \phi_{\beta}(\zeta).
\end{align*}
\]
d.: Show that $\phi_\beta = \phi_\gamma$ if and only if $\beta = \gamma$.

Suppose $\phi_\beta(\alpha) = \phi_\gamma(\alpha)$ for all $\alpha \in E$. Then $Tr(\beta \alpha) = Tr(\gamma \alpha)$, or $Tr((\beta - \gamma) \alpha) = 0$. If $\beta - \gamma \neq 0$, this last equation can only be true if the trace map is identically 0 (since we are allowed to choose $\alpha$ arbitrarily). However, the trace map can’t be identically 0 since any 0 of the trace map is a root of the polynomial $x^{p^n-1} + x^{p^n-2} + \cdots + x^p + x$, and there are at most $p^{n-1}$ roots out of the $p^n$ choices in $E$. This implies that $\phi_\beta$ and $\phi_\gamma$ are distinct.

e.: Recall that a linear transformation is completely determined by where it sends a basis for the vector space. Use this to count the number of distinct linear transformations from $GF(p^n)$ to $GF(p)$.

Since $[GF(p^n) : GF(p)] = n$, there is a basis $\{v_1, v_2, \ldots, v_n\}$ for $E$ over $GF(p)$. We are mapping each basis vector into $GF(p)$, so there are $p$ choices for each of the $n$ basis vectors giving a total of $p^n$ distinct linear transformations from $GF(p^n)$ to $GF(p)$.

f.: Use parts d. and e. to argue that all linear transformations are of the form $\phi_\beta$ for some $\beta \in E$.

We have $p^n$ choices for $\beta$, each of which yields a distinct linear transformation, and there are a total of $p^n$ linear transformations, so every linear transformation is of the form $\phi_\beta$ for $\beta \in GF(p^n)$. 