Module VI

Finite Fields This module deals with the existence and the structure of finite fields.

Remarks 1. $F[x]/(f(x))$ is a finite field when F is finite and f(x) is irreducible.

Proposition 1. If F is a finite field then $\exists$ a smallest number p, which is necessarily prime, such that $\forall a \in F$

$$p\,a \triangleq \underbrace{a + \cdots + a}_{\text{p times}} = 0$$

This number is called the characteristic of F and is denoted by ch(F).

Proof Consider any $a \in F - \{0\}$. Since F is finite the sequence a, a+a, a+a+a, $\cdots$, na, $\cdots$ must include a repetition, say

$$n\,a = m\,a$$

where n > m. Therefore (n-m)a = 0. Let n_a be the smallest positive integer such that

$n_a\ a = 1$

Claim $\forall$ a, b$\in$ F - $\{0\}$ $\quad (n_a = n_b)$

Proof $n_a\ b = n_a\left(ba^{-1}\right)a = ba^{-1}\ (n_a\ a)$ by the general distributive law of a field.

Hence

$$n_a b = ba^{-1}(0) = 0$$

and so $n_a \geq n_b$. Interchanging a and b yields $n_b \geq n_a$.

Denote the common value of the n_a's by p.

Claim p is prime

Proof If not $\exists$ 1 < r, s < p such that p = r s. Then

$$0 = p1 = r\,(s1)$$

Thus $r \geq p = n_{s1}$ if $s1 \neq 0$ - a contradiction. Hence s1 = 0.

But then $s \geq p = n_1$ - another contradiction.

Proposition 2. The elements $\{m\,\bar{1} \mid \ m = 0, 1, \ldots, p-1\}$ constitutes a subfield of F and the mapping

$$\psi: Z_p \rightarrow \{m\,\bar{1} \mid \ m = 0, 1, .., p-1\}$$
$$m \rightarrow m\,1$$

is an isomorphism, i.e. ψ is 1-1, onto and

$$\psi\,(n + m) = \psi\,(n) + \psi\,(m)$$
$$\psi\,(n\,m) = \psi\,(n)\;\psi\,(m)$$

for all m, n $\in$ Z_p i.e. $Z_p$and $\{m\,\bar{1} \mid m = 0, \ldots, p-1\}$ are algebraically identical.

Proof Observe that

$$m\,1 + n\,1 = (m+n)\,1 = r\,1$$

where

$$m + n = q\,p + r, 0 \leq r < p$$

Also

$$(m\,1)(n\,1) = (mn)1 = r'\,1$$

where

$$m\,n = q'\,p + r' \quad 0 \leq r' < p\,;$$

the operations are preserved. One-oneness and ontoness are obvious.

Remark 2. From this point on we "identify"

$$Z_p \text{ and } \{m\,1 \mid \ 0 \leq m \leq p-1\}$$

and regard Z_p as a subfield of F.

Remark 3. We shall see that if F is finite then $|F|$ is a power of the characteristic of F. The value of the exponent is a "vector space" parameter.

A Couple of Vector Space Essentials

Definition 1. A vector space V over a field F is a set V together with two operations:

$$+: V \times V \rightarrow V \text{ (called vector addition)}$$
$$(x, y) \rightarrow x + y$$

and $\bullet: F \times V \rightarrow V$ (called scalar multiplication)

$$(\alpha, x) \rightarrow \alpha \bullet x$$

such that (1) (V, +) is an abelian group

(2) $(\alpha\beta)\bullet x = \alpha\bullet(\beta\bullet x) \quad \forall \alpha,\beta \in F \ \ \forall x \in V$

(3) $(\alpha + \beta)\bullet x = \alpha\bullet x + \beta\bullet x \quad \forall \alpha,\beta \in F \ \forall x \in V$

$\alpha \bullet (x + y) = \alpha \bullet x + \alpha \bullet y \quad \forall \alpha \in F \quad \forall\, x, y \in V$

(4) $1 \bullet x = x \quad \forall\, x \in V$

Remark 4. We shall dispense with the "dot", i.e. we'll write αx instead of $\alpha \bullet x$.

Excercise 1: (Submit this one)

a) Prove: $0\, x = 0$, where the zero on the left is the additive identity of F and the zero on the right is the additive identity of V

b) Prove: $(-1)\, x = -x \ \forall x \in V$ where $-x$ is the additive inverse of x in $(V, +)$

c) Prove: $\alpha\, 0 = 0 \quad \forall \alpha \in F$

Definition 2. V is a finite dimensional vector space over F if and only if $\exists$ a finite set of vectors, say $x_1, .., x_n$ such that $\forall\, x \in V \ \exists\, a_1, \cdots, a_n \in F$ such that $x = \sum_{i=1}^{n} a_i x_i$ (linear combination; LC). The vectors $x_1 \cdots x_n$ are said to span V and $\{x_1, \cdots, x_n\}$ is a spanning set.

Example 1. $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ spans R^3 (3 - dimensional Euclidean space)

Example 2. $\{1, x, x^2\}$ spans $\{0, 1\}[x] / (x^3 + x + 1)$

Remark 5. In the previous two examples the coefficients required to write a particular x as a LC of the spanning vectors are seen to be unique - WHY?

Exercise 5. If F is any field then $F[x]$ is a vector space over F.

Prove it is NOT finite dimensional.

Definition 3. The set $\{x_1, .., x_n\} \subseteq V$ is linearly independent (LI) if and only if

$$\sum_{i=1}^{n} \alpha_i\, x_i = 0 \ \Rightarrow \ \alpha_i = 0 \ \forall i.$$

Otherwise the set is called linear dependent (LD).

Observation 1. $\{0 = x_1, x_2 .., x_n\}$ is LD

Proof $1\, 0 + 0\, x_2 + \cdot\cdot + 0\, x_n = 0.$

Proposition 3. The coefficients in the expression $\sum_{i=1}^{n} \alpha_i\, x_i$ are unique if and only if

$\{x_1, \cdot\cdot, x_n\}$ is LI.

Proof Of course $\sum_{i=1}^{n} \alpha_1 x_i = \sum_{i=1}^{n} \beta_i x_i \Leftrightarrow \sum_{i=1}^{n} (\alpha_i - \beta_i) x_i = 0.$

Thus if $\{x_1 \cdot\cdot, x_n\}$ is LI, $\alpha_i = \beta_i \ \forall_i$ (i.e. uniqueness) follows. Conversely if $\{x_1, \cdot\cdot, x_n\}$ is LD then $\exists\ \alpha_1, .., \alpha_n$ NOT ALL 0 such that

$$\sum_{i=1}^{n} \alpha_i x_i = 0.$$

Then $\sum_{i=1}^{n} (\alpha_i + \alpha_i) x_i = \sum_{i=1}^{n} \alpha_i x_i$, i.e. the coefficients are not unique.

Proposition 4. If $V \neq \{0\}$ and $S = \{x_1, x_2, \cdot\cdot, x_m\}$ is a spanning set for V then $S \supseteq B$ - a LI spanning set.

Proof (by induction on m) m = 1: if $S = \{x_1\}$ is a spanning set for V and $V \neq \{0\}$ then $x_1 \neq 0$ so suppose S is LD, i.e. $\exists \alpha \neq 0$ such that

$$\alpha x_1 = 0.$$

Then $\alpha^{-1}(\alpha x_1) = \alpha^{-1} 0 = 0$

i.e. $x_1 = 1 x_1 = (\alpha^{-1}\alpha) x_1 = 0$

Thus $\{x_1\}$ is LI.

Suppose the result is true for $|S| = m$ and consider the case where $|S| = m + 1$ i.e. $S = \{x_1, x_2 \cdot\cdot, x_m, x_{m+1}\}$

case (a) S is LI - then done!

case (b) S is LD: so $\exists\ \alpha_1 \cdot\cdot, \alpha_{m+1}$ NOT ALL sero such that

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_m x_m + \alpha_{m+1} x_{m+1} = 0$$

Now $\exists\ \alpha_j \neq 0$ so

$$x_j = \sum_{\substack{i=1 \\ i \neq j}}^{m+1} \alpha_j^{-1} \alpha_i x_i$$

Claim $S' = \{x_1, x_2, \cdot\cdot, x_j - 1, x_j + 1, \cdot\cdot, x_m + 1\}$ spans V

Indeed, if $x \in V\ \exists \beta_1, \cdot\cdot, \beta_{m+1}$ such that

$$\begin{aligned} x &= \sum_{i=1}^{m+1} \beta_1 x_1 = \sum_{i \neq j} \beta_i x_i + \beta_j x_j \\ &= \sum_{i \neq j} \beta_i x_i + \beta_j \left(\sum_{i \neq j} \alpha_j^{-1} \alpha_i x_i \right) \\ &= \sum_{i \neq j} (\beta_i + \beta_j \alpha_j^{-1} \alpha_i) x_i \end{aligned}$$

Thus, by the induction hypothesis, $S \supseteq S' \supseteq B$ where B is a LI spanning set

Definition 4 and Remark 6. A LI spanning set is called a basis. The proposition says that every spanning set of a finite dimensional vector space contains a basis. The proof shows that if the spanning set is LD it can be "pruned down" to a basis.

Our next objective is to prove that any two bases have equal size.

Proposition 5. If S is a spanning set for V and L is a LI set in V then $|L| \leq |S|$.

Proof Let $S = \{y_1, y_2, \cdot\cdot, y_m\}$ and $L = \{x_1, x_2, \cdot\cdot x_n\}$.

Claim If $L \underset{\neq}{\subset} S$ and $x_i \in L - S$ then $\exists\, y_j \in S - L$ such that

$$S - \{y_j\} \cup \{x_i\}$$

is a spanning set for V.

Proof Consider any $x_i \in L - S$. Since L is LI, $x_i \neq 0$.

Then $\exists$ non zero α_k, $k \in F \subseteq \{1, 2, \cdot\cdot m\}$ such that $x_i = \sum_{k \in F} \alpha_k\, y_k$.

Now not all the y_k can be in L for then $\sum_{k \in F} \alpha_k\, y_k + (-1)\, x_i = 0$

contradicts linear independence of L. Thus $\exists\, y_j \in S - L$ such that

$$y_j = \alpha_j^{-1} \Big(\sum_{\substack{k \neq j \\ k \in F}} (-\alpha_k)\, y_k + x_j\Big)$$

But then EVERY LC of vectors in S can be rewritten as a LC of the vectors in $S - \{y_j\} \cup \{x_i\}$. Exercise 3.

NOW SUPPOSE $m < n$. It follows by induction that $\{x_1, x_2 \cdot\cdot, x_m\}$ is a spanning set for V so that $x_{m+1} = \text{LC of } x_1, \cdot\cdot, x_m$ - this contradicts LI of L.

Note: This proof uses a "replacement" procedure.

Corollary 2 and Definition 5. Any two bases for V have the same size. That size is referred to as the dimension of V and is denoted by dim V.

Proof Suppose B_1 and B_2 are bases. Since B_1 is LI and B_2 is a spanning set $|B_1| \leq |B_2|$. Likewise, since B_2 is LI and B_1 is a spanning set $|B_2| \leq |B_1|$.

Exercise 4. (Submit d) Suppose V is finite dimensional with dimV = n.

a) Prove: If B is LI and $|B| = n$ then B is a basis for V.

b) Prove: IF S is a spanning set for V and $|S| = n$ then S is a basis for V.

c) Prove: If $L \subseteq V$ is LI then $\exists$ a basis B for V such that $L \subseteq B$.

d) Prove: If W is also a vector space over F with dim V = n then V and W are (vector space) isomorphic ie. $\exists$

$T\colon V \to W$

such that T is a bijection and $T(\alpha x+y) = \alpha T(x) + T(y)\ \forall \alpha \in F,\ x,\ y \in V$.

Hint Let $\{x_1, \cdot\cdot, x_n\}$ be a basis for V and $\{w_1,\ w_2, \cdot\cdot, w_n\}$ be a basis for W. Define

$$T\left(\sum_{i=1}^{n} \alpha_1\, x_i\right) = \sum_{i=1}^{n} \alpha_i\, w_i$$

Theorem 1. If F is a finite field with chF=p then F is a finite dimensional vetor space over Z_p. Furthermore, if $\dim F = k$ then $|F| = p^k$

Proof The vector space sum is just the sum in F; scalar multiplication is given by $m \cdot a = (m1)a$ where the multiplication on the right is field multiplication. The properties of a vector space are easy to verify. Since F is finite ∃ a finite spanning set for F so that F is finite dimensional. If $\{\alpha_1,\ \alpha_2, \cdot\cdot,\ \alpha_k\}$ is a basis then the elements of F are uniquely represented in the form $\alpha = \sum_{i=1}^{k} m_i \cdot \alpha_i$

As there are p choices for each m_i it follows that $|F| = p^k$

Example 2 revisited. The elements 1, x and x^2 constitute a basis for $F[x]/\ (f(x))$ where $F = Z_2 = \{0, 1\}$ and $f(x) = x^3 + x + 1$, i.e. $m_1\ 1 + m_2\ x + m_3\ x^2$ runs through all of $\{0, 1\}[x]/\ (x^3 + x + 1)$ as $m_1,\ m_2$ and m_3 run through $Z_2 = \{0, 1\}$.

Also $\left|\{0,1\}[x]/(x^3 + x + 1)\right| = 2^3 = 8$ as we have already seen.

Remark 7. If F and G are two finite fields such that $|F| = |G|$ then with $|F| = p^k$ and $|G| = q^\ell$ it follows that $p = q$ and $k = \ell$. Hence F and G are k-dimensional vector spaces over Z_p and are therefore vector space isomorphic; however the isomorphism doesn't necessarily preserve "field" multiplication. As it happens F and G are "field" isomorphic but we require some additional insights before we prove this fact.

One fundamental insight has already been discovered in Module III.

Theorem 2. If F is a finite field then the multiplicative group $F^* = F - \{0\}$ is cyclic; i.e. $\exists \alpha \in F^*$ such that $F = \{1 = \alpha^\circ, \alpha^1, \cdot\cdot, \alpha^{p^k - 2}\}$.

Exercise 5. (Submit this one) a) Prove that the number of primitive elements (i.e. generators) in F^* is just $\varphi(p^k - 1)$. If α is a given primitive then $\{\alpha^t \mid \gcd(t, p^k - 1) = 1\}$ is the collection of all primitives.

b) Prove α is a primitive if and only in $\forall$ primes q

$$\left(\text{if } q \mid p^k - 1 \text{ then } \alpha^{\frac{p^k - 1}{q}} \neq 1\right)$$

Exercise 6. Consider $\{0, 1\}[x]/\ (x^3 + x + 1)$.

How many primitives does this field have? Find them.

Example 3. Consider $\{0, 1\}[x]/\ (x^4 + x^3 + x^2 + x + 1)$

Claim This is a field as $x^4 + x^3 + x^2 + x + 1$ is irreducible.

Proof Since neither 0 nor 1 is a root x+1 and x are not factors. Consider

$$(x^2 + \alpha x + \beta)(x^2 + \psi x + \partial) = x^4 + x^3 + x^2 + x + 1$$

Since $1, x, x^2, x^3$ is a basis we get

$\beta \partial = 1$ i.e. $\beta = \partial = 1$

Thus $\alpha \partial + \psi \beta = 1$, i.e. $\alpha + \psi = 1$

We logically assume $\alpha = 1$, $\psi = 0$. Then $\partial + \alpha \psi + \beta = 1$

But $\partial + \alpha \psi + \beta = 0 \neq 1$. Thus the polynomial is irreducible.

Since $|F^*| = 2^4 - 1 = 15$ there are $\varphi(15) = 8$ primitives.

Observe $x^4 = x^3 + x^2 + x + 1$

so $x^5 = x^4 + x^3 + x^2 + x = x^3 + x^2 + x + 1 + x^3 + x^2 + x = 1$

Thus ord (x) = 5. Next consider x + 1:

$$(x + 1)^2 = x^2 + 1$$

$$(x + 1)^3 = x^3 + x^2 + x + 1 = x^4$$

$$(x + 1)^4 = x^5 + x^4 = 1 + x^3 + x^2 + x + 1$$
$$= x^3 + x^2 + x$$

$$(x + 1)^5 = x^3 + x^2 + 1 \neq 1$$

Thus (ord) (x+1) = 15.

The other primitives are

$$(x+1)^2 = x^2 + 1$$
$$(x+1)^4 = x^3 + x^2 + x$$
$$(x+1)^7 = \left(x^2+1\right)\left(x^3+x^2+1\right) = x^2 + x + 1$$
$$(x+1)^8 = x^3 + 1$$
$$(x+1)^{11} = \left(x+1\right)^3\left(x+1\right)^8 = x^3 + x + 1$$
$$(x+1)^{13} = x^2 + x$$

and $(x+1)^{14} = x^3 + x$.

Corollary 2.1 Every element of F^* is a root of $x^{p^k-1} - 1$; in fact

$x^{p^k} - x = x\prod_{i=0}^{p^k-2}\left(x - \alpha^i\right)$ where α is a primitive.

Remark 8. The previous corollary shows that for each $\beta \in F^*$ $\exists$ a monic polynomial in $Z_p[x]$, i.e. with coefficients from Z_p, that β satisfies.

Definition 6. If $\beta \in F$ then the minimal polynomial of β is THE monic polynomial $M(x) \in Z_p[x]$ of SMALLEST degree having β as a root.

Remark 9. That $M_\alpha(x)$ is unique is left to Exercise 7.

Theorem 3. If $\beta \neq 0$ then $M_\beta(x) \mid x^{p^k-1} - 1$. Furthermore $M_\beta(x)$ is irreducible in $Z_p[x]$.

Proof Write $x^{p^k-1} - 1 = q(x)\,M(x) + r(x)$ $\deg r < \deg M_\beta$ in $Z_p[x]$ by the Division Algorithm.

But $r(\beta) = 0$

Now r(x) cannot be a non-zero constant and, since $M_\beta(x)$ has the minimum degree such that $M_\beta(\beta) = 0$, r must be the zero polynomial.

Next suppose $M_\beta(x) = P(x)\,Q(x)$ where P and Q are monic and of positive degree.

But $0 = M_\beta(\beta) = P(\beta)\;Q(\beta)$ in F so $P(\beta) = 0$ or $Q(\beta) = 0$ - which contradicts the definition of $M_\beta(x)$.

Exercise 8. (Submit this one)

a) Suppose $f(x) \in Z_p[x]$ and $f(\alpha) = 0$; prove $M_\alpha \mid f$ (Hint: Immitate the proof of the previous theorem).

b) Prove: M_α is unique

c) Prove: If $f(x) \in Z_p[x]$, is irreducible, monic and $f(\alpha) = 0$ then $f(x) = M_\alpha(x)$

d) What is the minimal polynomial of 0?

Our next major task is to prove that any two finite fields having the same number of elements are FIELD isomorphic but first we require lemmas, the second of which is essential for the definition of the isomorphism.

Our first lemma is a very useful technical lemma and is concerned with the coefficients of the polynomial $(f(x))^p$ where $f(x) \in F[x]$ and chF =p.

Lemma1. Let F be a finite field with chF = p

(1) if $g(x), h(x) \in F[x]$ then $(g(x) + h(x))^p = (g(x))^p + (h(x))^p$

(2) if $f(x) = \sum_{i=0}^{n} a_i x^i$ then $(f(x))^p = \sum_{i=0}^{n} a_i^p (x^p)^i$.

(3) if $F = Z_p$ and $f(x) \in Z_p[x]$ then $(f(x))^p = f(x^p)$

Proof (1) It is a technical exercise to prove

$$(g(x) + h(x))^p = \sum_{i=0}^{p} \binom{p}{i} (g(x))^i (h(x))^{p-i}$$

Since $p \Big| \binom{p}{i}$ for $1 \le i \le p - 1$ it follows that $\binom{p}{i} 1 = 0$ for i = 1,.., p-1 and the result follows.

(2) The use of induction and (1) yields (2).

(3) In this case $a^p = a \ \forall a \in Z_p$ (Euler's Theorem).

so the conclusion follows from (2).

Lemma 1. Suppose $|F| = |G| = p^k$, α is a primitive of F^* and $M_\alpha(x) \in Z_p[x]$ is the minimal polynomial of α.

Then

(1) $\exists \beta \in G$ such that $M_\alpha(x)$ is the minimal polynomial of β,

(2) every root of $M_\alpha(x)$ in G, in particular the β of (1), is a primitive in G^*

and (3) the roots of $M_\alpha(x)$ in F are given by $\alpha, \alpha^p, ..., \alpha^{p^{k-1}}$ and $M_\alpha(x) = \prod_{i=1}^{k-1} (x - \alpha^{p^i})$ in $F[x]$;

likewise the roots of $M_\alpha(x)$ in G are given by $\beta, \beta^p, ..., \beta^{p^{k-1}}$ and $M_\alpha(x) = \prod_{i=1}^{k-1} \left(x - \beta^{p^i}\right)$ in $G[x]$.

Proof (1) Recall from Theorem 3 that $M_\alpha(x) \Big| \ x^{p^k-1} - 1$. Thus $\exists N(x) \in Z_p[x]$ such that

$$x^{p^k-1} - 1 = M_\alpha(x) N(x)$$

Now, focusing on G, it follows by Corollary 2.1 that EVERY element of G^* is a root of $x^{p^k-1} - 1$. Hence if $\beta \in G^*$ then $M_\alpha(\beta) N(\beta) = 0$ so that either β is a root of $M_\alpha(x)$ or β is a root of N(x). By Theorem 3 of Module V N(x) can have no more that deg N roots in G. But

$$\text{deg } N = p^k - 1 - \text{deg } M_\alpha < p^k - 1 \text{ so } \exists \beta \in G \text{ such that } \beta \text{ is a root of } M_\alpha(x).$$

(2) Let φ denote an arbitrary root of M_α (x) in G. As $M_\varphi(x)$ and $M_\alpha(x)$ are irreducible in $Z_p[x]$ by Theorem 3 and $M_\varphi(x) \mid M_\alpha(x)$ by Exercise 7 c) it follows that $M_\alpha(x)$ is the minimal polynomial of φ. Thus, by a) of Exercise 8.

$$M_\alpha(x) \mid x^{\operatorname{ord}\varphi} - 1$$

and so

$$\alpha^{\operatorname{ord}\varphi} - 1 = 0$$

because $M_\alpha(\alpha)$=0. But ord $\alpha = p^k - 1$ so $p^k - 1 \mid$ ord φ

Finally then ord$\varphi \mid p^k - 1$ because $|G^*| = p^k - 1$ and ord $\varphi = p^k - 1$

(3) Now Lemma 1 (3) yields $(M_\alpha(x))^p = M_\alpha(x^p)$ so the fact that $M_\alpha(\alpha) = 0$ implies that $M_\alpha(\alpha^p) = 0$. Thus by induction. $M_\alpha(\alpha^{p^i}) = 0$ $\forall i \geq 0$. Consider the powers $\alpha, \alpha^p, \alpha^{p^2}, .., \alpha^{p^{k-1}}$; we claim that they are distinct. Indeed, if $\alpha^{p^i} = \alpha^{p^j}$ where $0 \le i \le j \le$ k-1 then $\alpha^{p^j - p^i} = 1$. But then $p^k - 1 = \text{ord } \alpha \mid p^j - p^i$ - a contradiction since $p^j - p^i < p^k - 1$.

Next realize that the distinctness implies that $x - \alpha, x - \alpha^p, ..., x - \alpha^{p^{k-1}}$ are pairwise relatively prime irreducible polynomials, each of which divides $M_\alpha(x)$ by Theorem 3 of Module V. Thus

$$\prod_{1=0}^{k-1} (x - \alpha^{p^i}) \mid M_\alpha(x).$$

Of course, the required conclusion follows from the fact that deg $M_\alpha \le$ k.

To see this observe that $\{1, \alpha, \alpha^2, .., \alpha^k\}$ is LD in F (since dimF = k), i.e.

$\exists$ $a_0, .., a_k$ such that $\sum_{i=0}^{k} a_i \alpha^i = 0$ and not all $a_i = 0$. Thus $\exists$ a polynomial of deg $\le$ k that has α as a root. But then deg $M_\alpha \le$ k follows.

The argument for β is identical to this one.

Exercise 9. (Submit a; b is for extra credit)

a) With F as in Lemma 2 and α a primitive of F^*, prove that

$\alpha^p, \alpha^{p^2}, .., \alpha^{p^{k-1}}$ are also primitives.

b) Suppose F is finite with chF = p and consider $M_\varphi(x) \in Z_p[x]$ where $\varphi \in F^*$.

Prove: if $\alpha \in F^*$ is a root of $M_\varphi(x)$ then ordφ = ordα

Theorem 4. If $\left[\mathrm{F}\right] = \left|\mathrm{G}\right| = \mathrm{p}^{\mathrm{k}}$ then F and G are field isomorphic. More specifically, if α is a primitive in F^{*} with minimal polynomial $\mathrm{M}_{\alpha}(\mathrm{x}) \in \mathrm{Z}_{\mathrm{p}}\left[\mathrm{x}\right]$ and β is a root of $\mathrm{M}_{\alpha}(\mathrm{x})$ in G then

$$\psi\colon \mathrm{F} \to \mathrm{G}$$

$$\mathrm{a} \to \psi(\mathrm{a}) = \begin{cases} 0 & \text{if } \mathrm{a} = 0 \\ \beta^{\mathrm{j}} & \text{if } \mathrm{a} = \alpha^{\mathrm{j}},\ 0 \le \mathrm{j} \le \mathrm{p}^{\mathrm{k}} - 2 \end{cases}$$

is a bijection such that

(i) $\psi(\mathrm{a}+\mathrm{b}) = \psi(\mathrm{a}) + \psi(\mathrm{b})$

(ii) $\psi(\mathrm{ab}) = \psi(\mathrm{a}) \cdot \psi(\mathrm{b})$

Proof Consider ψ as given.

Claim 1. ψ is 1-1: Suppose $\mathrm{a} \ne \mathrm{b}$. If $\mathrm{a}, \mathrm{b} \in \mathrm{F}^{*}$ then $\mathrm{a} = \alpha^{\mathrm{i}}$ and $\mathrm{b} = \alpha^{\mathrm{j}}$ where $\mathrm{i} \ne \mathrm{j}$ and $0 \le \mathrm{i}, \mathrm{j} \le \mathrm{p}^{\mathrm{k}} - 2$. But then, since β is a primitive of G^{*} by Lemma 2(2)

$$\psi(\mathrm{a}) = \beta^{\mathrm{i}} \ne \beta^{\mathrm{j}} = \psi(\mathrm{b})$$

if $\mathrm{a} = 0$ and $\mathrm{b} = \alpha^{\mathrm{j}}$ then

$$\psi(\mathrm{a}) = 0 \ne \beta^{\mathrm{j}} = \psi(\mathrm{b})$$

Claim 2. ψ is onto: Consider $\mathrm{c} \in \mathrm{G}$. Then either $\mathrm{c} = 0$ or $\mathrm{c} = \beta^{\mathrm{j}}$ where $0 \le \mathrm{j} \le \mathrm{p}^{\mathrm{k}} - 2$ by Lemma 2(2). Thus

$$\psi(0) = 0 = \mathrm{c} \text{ or } \psi(\alpha^{\mathrm{j}}) = \beta^{\mathrm{j}} = \mathrm{c}.$$

Claim 3. ψ satisfies ii): Consider

$$\begin{aligned} \psi\left(\alpha^{\mathrm{i}}\ \alpha^{\mathrm{j}}\right) &= \psi\left(\alpha^{\mathrm{i+j(mod\ p^{k}-1)}}\right) \\ &= \beta^{\mathrm{i+j(mod\ p^{k}-1)}} \\ &= \beta^{\mathrm{i}}\ \beta^{\mathrm{j}} = \psi\left(\alpha^{\mathrm{i}}\right)\ \psi\left(\alpha^{\mathrm{j}}\right) \end{aligned}$$

Also

$$\psi(0 \cdot \mathrm{a}) = \psi(0) = 0 = 0 \cdot \psi(\mathrm{a}) = \psi(0)\ \psi(\mathrm{a})$$

Claim 4. ψ satisfies $i)$: First consider

$$\psi(0+\mathrm{b}) = \psi(\mathrm{b}) = 0 + \psi(\mathrm{b}) = \psi(0) + \psi(\mathrm{b})$$

Next suppose a, b $\neq 0$ but a+b = 0. Then $\mathrm{a} = \alpha^{\mathrm{i}}$, $\mathrm{b} = \alpha^{\mathrm{j}}$
so that

$$\alpha^{\mathrm{i}} + \alpha^{\mathrm{j}} = 0$$

and α is a root of $\mathrm{f(x)} = \mathrm{x}^{\mathrm{i}} + \mathrm{x}^{\mathrm{j}} \in \mathrm{Z}_{\mathrm{p}}[\mathrm{x}]$. Now it follows by Exercise 7(a) that $\mathrm{M}_\alpha(\mathrm{x}) \mid \mathrm{f(x)} = \mathrm{x}^{\mathrm{i}} + \mathrm{x}^{\mathrm{j}}$. But $\mathrm{M}_\alpha(\beta) = 0$ by Lemma 2(2) so

$$0 = \mathrm{f}(\beta) = \beta^{\mathrm{i}} + \beta^{\mathrm{j}}$$

and so

$$\psi(\mathrm{a}+\mathrm{b}) = \psi(0) = 0 = \beta^{\mathrm{i}} + \beta^{\mathrm{j}} = \psi(\mathrm{a}) + \psi(\mathrm{b})$$

Exercise 9. (Extra credit) Prove $i)$ for the case a, b, and a + b $\neq$ 0.

Remark 9. The existence of the field isomorphism means that F and G are "algebraically" identical. Indeed, the function ψ merely renames the elements of F, e.g. $\psi(0)$ is the additive identity of G, $\psi(\text{-a})$ is the additive inverse of $\psi(\mathrm{a})$ in G, $\psi(1)$ is the multiplicative identity in G and $\psi(\mathrm{a}^{-1})$ is the multiplicative inverse of $\psi(\mathrm{a})$ when a $\neq 0$.

Corollary 4.1 If $|\mathrm{F}| = \mathrm{p}^{\mathrm{k}}$, α is a primitive of F^* and $\mathrm{M}_\alpha(\mathrm{x})$ is the minimal polynomial of α then

$$\hat{\psi}\colon \mathrm{F} \to \mathrm{Z}_{\mathrm{p}}[\mathrm{x}] \,/\, (\mathrm{M}_\alpha\ (\mathrm{x}))$$

$$\mathrm{a} \to \hat{\psi}(\mathrm{a}) = \begin{cases} 0 \text{ if } \mathrm{a} = 0 \\ \mathrm{x}^{\mathrm{j}} \text{ if } \mathrm{a} = \alpha^{\mathrm{j}},\ \ 0 \leq \mathrm{j} \leq \mathrm{p}^{\mathrm{k}} - 2 \end{cases}$$

is a field isomorphism.

Proof It is enough to note that $\left|\mathrm{Z}_{\mathrm{p}}[\mathrm{x}] / (\mathrm{M}_\alpha(\mathrm{x}))\right| = \mathrm{p}^{\mathrm{k}}$ and $\mathrm{M}_\alpha(\mathrm{x}) = 0$ (mod $\mathrm{M}_\alpha(\mathrm{x})$), i.e. x is a root of M_α in $\mathrm{Z}_{\mathrm{p}}[\mathrm{x}] / (\mathrm{M}_\alpha(\mathrm{x}))$ for then the result follows from Theorem 5 with $\mathrm{G} = \mathrm{Z}_{\mathrm{p}}[\mathrm{x}] / (\mathrm{M}_\alpha(\mathrm{x}))$ and $\beta = \mathrm{x}$.

Example 4. Consider $\mathrm{F} = \mathrm{Z}_2[\mathrm{x}] / \left(\mathrm{x}^4 + \mathrm{x}^3 + \mathrm{x}^2 + \mathrm{x} + 1\right)$

Of course

$$\mathrm{M}_{\mathrm{x}}(\mathrm{y}) = \mathrm{y}^4 + \mathrm{y}^3 + \mathrm{y}^2 + \mathrm{y} + 1$$

is the minimal polynomial of the ELEMENT $\mathrm{x} \in \mathrm{F}$. However x is NOT a primitive of F for as it was shown in Example 3, $\mathrm{x}^5 = 1$. It was also shown in that example that x + 1 is a primitive.

Observe that

$$\left(x+1\right)^{4}=x^{4}+1=x^{3}+x^{2}+x$$

and $$\left(x+1\right)^{3}=x^{3}+x^{2}+x+1$$

so

$$\left(x+1\right)^{4}+\left(x+1\right)^{3}+1=0$$

But it is easily shown that $y^{4}+y^{3}+1$ is irreducible in $Z_2\left[y\right]$ so it follows by Exercise 7 (c) that

$$M_{x+1}(y)=y^{4}+y^{3}+1$$

Thus

$$\begin{aligned} \psi\colon Z_2\left[x\right]/\left(x^{4}+x^{3}+x^{2}+x+1\right) &\rightarrow Z_2\left[y\right]/\left(y^{4}+y^{3}+1\right) \\ a &\rightarrow \psi(a)=\begin{cases} 0, \text{ if } a=0 \\ y^{i}, \text{ if } a=(x+1)^{j},\ 0\leq j\leq 1 \end{cases} \end{aligned}$$

is an isomorphism.

Definition 7. If $M(x)$ is a monic irreducible polynomial in $Z_p\left[x\right]$ and x is a primitive (generator) of $Z_p\left[x\right]/\left(M(x)\right)^{*}$ then $M(x)$ is called a primitive polynomial.

Remark 10 and Example 4 revisited: Not every irreducible polynomial is primitive. Consider $F=Z_2\left[x\right]/\left(x^{4}+x^{3}+x^{2}+x+1\right)$; then $x^{4}+x^{3}+x^{2}+x+1$ is NOT primitive since x is not a generator. Recall that $x+1$ is a generator of F^{*} and $M_{x+1}(y)=y^{4}+y^{3}+1$. Thus, by the result of the example, $x^{4}+x^{3}+1$ is primitive.

Exercise 10. (Submit this one) a) Prove directly that x is a generator of $Z_2\left[x\right]/\left(x^{4}+x^{3}+1\right)$

b) Prove: $x^{4}+x+1\in Z_2\left[x\right]$ is primitive.

Example 4. revisited again: Now

$$x^{15}+1=\left(x^{4}+x^{3}+x^{2}+x+1\right)\left(x^{4}+x^{3}+1\right)\left(x^{4}+x+1\right)\left(x^{2}+x+1\right)\left(x+1\right)$$ so, of the three irreducible factors of $x^{15}+1$ in $Z_2\left[x\right]$ of degree four, two are primitive.

Remark 11. Motivated by the previous example we shall study the factorization of $x^{p^k}-x$ over $Z_p\left[x\right]$ next. This study will enable us to conclude that for EVERY positive integer k $\exists$ a monic irreducible polynomial of degree k in $Z_p\left[x\right]$. In preparation for this result we obtain a useful number-theoretic lemma.

Lemma 3. If $n\geq 2$ and $s\geq r\geq 1$, then $n^{r}-1\mid n^{s}-1$ if and only if $r\mid s$.

Proof Observe that if $r|s$ then $s = mr$ and

$$n^s - 1 = \left(n^r - 1\right)\left(n^{(m-1)r} + n^{(m-2)r} + \cdots + n^r + 1\right)$$

so $n^r - 1 | n^s - 1$.

Conversely, suppose $n^r - 1 | n^s - 1$ and write

$$s = q\,r + t$$

where $t < r$. Then

$$n^s - 1 = n^{qr+t} - 1 = n^{qr+t} - n^t + n^t - 1$$
$$= n^t\left[n^{qr} - 1\right] + n^t - 1$$

Now by the first part of the argument $n^r - 1 | n^{qr} - 1$

and so

$$n^r - 1 | n^t - 1$$

As $0 \le t < r$ we see that $t = 0$.

Exercise 11. (Submit this one) Prove: If F is ANY field then

$$x^m - 1 | x^n - 1 \quad \text{in } F[x] \text{ if and only if } m|n.$$

Theorem 5. Let p be prime and $k \ge 1$. Then

(a) an irreducible polynomial $f(x) \in Z_p[x]$ divides $x^{p^k} - x$ if and only if $\deg f | k$;

(b) $x^{p^k} - 1$ is the product of ALL monic irreducible polynomials from $Z_p[x]$ having degree that divides k.

Proof (a) Consider $F = Z_p[x]/(f(x))$ where $f(x) \neq x$. Of course $|F| = p^{\deg f}$. Now $f(x)$ is the minimal polynomial of x in F so by Theorem 3

$$f(x) \mid x^{p^{\deg f\text{-}1}} - 1$$

But $\deg f \mid k$ implies $p^{\deg f} - 1 \mid p^k - 1$ by Lemma 2 and this in turn forces

$$x^{p^{\deg f} - 1} - 1 \mid x^{p^k - 1} - 1$$

by Exercise 11. Hence $f(x) \mid x^{p^k - 1} - 1$.

Conversely, suppose $f(x) \mid x^{p^k - 1} - 1$ and again consider $F = Z_p[x]/(f(x))$. Let α be a primitive of F and write

$$\alpha = a_0 + a_1 + \cdot\cdot + a_d\, x^d$$

where $d =$ deg f and $a_0, a_1, \ldots, a_d \in Z_p$. Then, by Lemma (3)

$$\alpha^{p^k} = \sum_{i=0}^{d} a_i \left(x^{p^k}\right)^i \qquad \text{in } F$$

But $f(x) \mid x^{p^k} - x$ and $f(x) = 0$ in F force $x^{p^k} = x$ in F.

Thus $\alpha^{p^k} = \alpha$ and $\alpha^{p^k - 1} = 1$. Hence

$$\text{ord}\,\alpha = p^d - 1 \mid p^k - 1$$

from which it follows by Lemma 2 that $\deg f = d \mid k$.

Proof (b) We know from Theorem 3 of Module V that

$$x^{p^k} - x = \prod_{i=1}^{m} (f_i(x))^{e_i}$$

where $f_1, f_2, .., f_m$ are distinct monic irreducible polynomials from $Z_p[x]$ and $e_1, e_2, .., e_m$ are positive integers. We claim that each $e_i = 1$. Indeed, suppose some $e_i \geq 2$. Then

$$x^{p^k} - x = (f_i(x))^2\ N(x)$$

where $N(x) \in Z_p[x]$. Now it is the case that the ordinary algebraic rules of differentiation of polynomials hold for $Z_p[x]$ but we defer the verification of these rules to Appendix I (for the interested reader).

Hence

$$\left(p^{k}1\right)\ x^{p^{k}-1} - 1 \ = \ 2\left(f_i(x)\right)\ N(x) + \left(f_i(x)\right)^2\ N'(x) \text{ or, equivalently,}$$

$$- 1 = 2\left(f(x)\right)\ N(x) + \left(f_i(x)\right)^2\ N'(x)$$

Thus $f_i(x) \big| \ - \ 1$ (even if $p = 2$ and/or $N'(x) = 0$) - a contradiction.

Therefore

$$x^{p^k} - x \ = \ \prod_{i=1}^{m} f_i(x)$$

Of course $\deg f_i \big| k$ for each i by (a) of this theorem. Moreover, if $f(x)$ is monic and irreducible with k divisible by $\deg f$ then

$$f(x) \big| \ x^{p^k} - x = \prod_{i=1}^{m} f_i(x)$$

Thus, it follows by Proposition 4 of Module V that $f(x) = f_i(x)$ for some $1 \leq \ 1 \leq m$ and the proof is complete.

<u>Corollary 5.1</u> and <u>Remark 12</u>. Let $d \big| k$ and denote by $I_p(d)$ the number of monic irreducible polynomials in $Z_p\left[x\right]$ having the degree d. Then

$$p^k = \sum_{d|k} d\, I_p(d)$$

With the aid of "Mobius inversion", to be presented in a subsequent lemma, we shall obtain a formula for $I_p(k)$. Then by using some simple inequalities we will show that $I_p(k) > 0\ \forall$ primes p and $\forall\ k \geq\ 1$.

<u>Proof</u> It is enough to note that $d\, I_p(d)$ is the contribution of the monic irreducible polynomials having degree d to the degree of $x^{p^k} - 1$. Then the formula follows by b) of Theorem 5.

<u>Definition 8</u>. (Mobius μ Function) The function

$$\mu\colon\ Z^+ \ \rightarrow\ \left\{-1, 0, 1\right\}$$

$$n \quad \rightarrow \ \mu(n) = \begin{cases} 1 \text{ if } n = 1 \\ (-1)^r \text{ if } n = p_1\, p_2 \cdots\, p_r \\ 0 \text{ otherwise} \end{cases}$$

where $p_1, ..., p_r$ are distinct primes, is referred to as the Mobius μ function.

A salient technical property is given next

<u>Lemma 4</u>. $\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ otherwise} \end{cases}$

<u>Proof</u> Of course, if n = 1 the result holds.

Suppose $n \geq 2$, so that $n = p_1^{e_1} p_2^{e_2} \cdot\cdot p_k^{e_k}$. Then $d|n$ if and only if $d = p_1^{t_1} p_2^{t_2} \cdot\cdot p_k^{t_k}$ where $0 \leq t_i \leq e_i$. Now if any $t_i \geq 2$, $\mu(d) = 0$ so

$$\sum_{d|n} \mu(d) = 1 + \sum_{r=1}^{k} \sum_{pi_1,\cdot\cdot pi_r} (-1)^r$$

$$= 1 + \sum_{r=1}^{k} \binom{k}{r} (-1)^r$$

$$= (1 + (-1))^k = 0$$

by the Bimomial Theorem.

<u>Lemma 5</u>. (<u>Mobius Inversion</u>) Consider two real-valued functions f and g defined on Z^+ related by the expression

$$f(n) = \sum_{d|n} g(d) \qquad \forall\, n \geq 1$$

Then

$$g(n) = \sum_{d|n} \mu(d)\; f\left(\frac{n}{d}\right) \quad \forall\, n \geq 1$$

<u>Proof</u> Consider

$$\sum_{d|n} \mu(d)\, f\left(\frac{n}{d}\right) = \sum_{d|n} \sum_{d'|\frac{n}{d}} \mu(d)\, g(d')$$

Now $d|n$ and $d'\Big|\frac{n}{d}$ if and only if $d'|n$ and $d\Big|\frac{n}{d'}$ so

$$\sum_{d|n} \mu(d)\, f\left(\frac{n}{d}\right) = \sum_{d'|n} g(d') \sum_{d|\frac{n}{d'}} \mu(d)$$

But

$$\sum_{d|\frac{n}{d'}} \mu(d) = 0 \text{ if } d'|n \text{ and } d' < n$$

Thus

$$\sum_{d|n} \mu(d)\, f\left(\frac{n}{d}\right) = g(n)$$

and the proof is complete.

Theorem 6. $\forall$ primes p $\forall$ $k \le 1$ ($\exists$ a monic irreducible polynomial of degree k in $Z_p[x]$). Consequently $\exists$ an algebraically unique finite field of order p^k, namely $Z_p[x]/(f(x))$, where f(x) is a monic irreducible polynomial of degree k from $Z_p[x]$. We use the notation G F (p^k) to denote this field.

Proof By Corollary 5.1 and Lemma 4

$$\begin{aligned} I_p(k) &= \sum_{d|k} \mu(d)\, p^{\frac{k}{d}} \\ &= p^k + \sum_{d|k,\, d>1} \mu(d)\, p^{\frac{k}{d}} \\ &\ge p^k - \sum_{i=1}^{k-1} p^i > p^k - \left(\frac{p^k - 1}{p-1}\right) > 0 \end{aligned}$$

Hence $\exists$ such a polynomial in $Z_p[x]$.

Remark 13. and Exercise 12. (Submit this one) The Mobius μ function and Mobius Inversion are important number-theoretic topics with many applications, in addition to the application given here. Consult Appendix II for two more. Furthermore, the Mobius function and the Euler -φ function are related as follows:

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

a) Prove this. Hint: Write $\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$, where $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, and expand the product

b) Prove (using Mobius inversion):

$$n = \sum_{d|n} \varphi(d).$$

In the remainder of this module we study the structure of $GF(p^k)$. Specifically, we determine which finite fields $GF(p^{\ell})$ are subfields of $GF(p^k)$.

Proposition 6. If $GF(p^{\ell})$ is a subfield of $GF(p^k)$ then $\ell \mid k$.

Proof Consider a primitive $\alpha \in GF(p^{\ell})^*$. Since $\alpha \in GF(p^k)^*$ as well

$$p^{\ell} - 1 = \text{ord}\,\alpha \mid \left|GF(p^k)^*\right| = p^k - 1$$

Thus $\ell \mid k$ by Lemma 3.

The converse requires a little more work.

Proposition 7. If $\ell \mid k$ then $GF(p^{\ell})$ is a subfield of $GF(p^k)$.

Proof Since $GF(p^k)^*$ is cyclic and $p^{\ell} - 1 \mid p^k - 1$ by Lemma 2, $GF(p^k)^*$ has a unique cyclic subgroup of order $p^{\ell} - 1$, say H. It is enough to prove that $H \cup \{0\}$ is a subgroup of $(GF(p^k), +)$. To do this consider $a, b \in H \cup \{0\}$. Since $a - b \in H \cup \{0\}$ trivially if either a or b = 0 suppose $a = \alpha^i$ and $b = \alpha^j$ where α is a primitive of H. Now

$$(a - b)^{p^{\ell}} = a^{p^{\ell}} - b^{p^{\ell}}.$$

(Proof: Exercise 13.)

and, since $a^{p^{\ell}} = a$ and $b^{p^{\ell}} = b$ by Euler's Theorem and induction it follows that

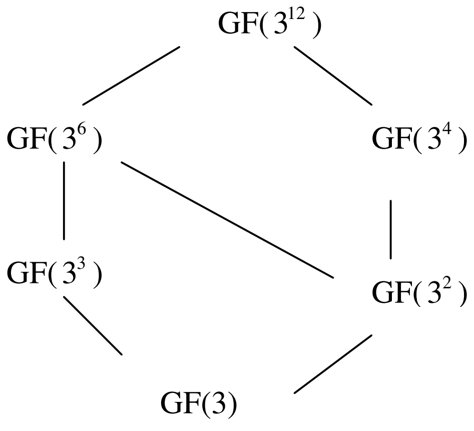
$$(a - b)^{p^{\ell}} = a - b.$$

Thus, if $a \neq b$

$$(a - b)^{p^{\ell} - 1} = 1$$

and, because H contains ALL elements having order that divides $p^{\ell} - 1$, $a - b \in H$. Of course if $a = b$ $\quad a - b = 0 \in H \cup \{0\}$.

Example 5. We draw a hierarchical diagram of the subfield structure of $GF(3^{12})$ indicating subfield inclusions:



Exercise 14. (Submit this one) Detrmine the subfields of GF(5^{100}) and draw a hierarchical diagram indicating subfield inclusions.