1. Let $F$ be as in Example 1 (on page 383). Use the generator $z = x^2 + 1$ for $F^\#$ and construct a table that convert polynomials in $F^\#$ to powers of $z$, and vice versa. Here $F^\#$ means the nonzero elements of the field $F$.

**Answer:** The conversion table can be constructed using the following maple commands:

```maple
given = x --> x^4 + x + 1;
generate := x^2 + 1;
for i from 1 to 15 do
    temp := Powmod(generate, i, given(x), x) mod 2;
    print(x^i, ' field element ', temp);
end do;
```

Of course you can do this by hand proceeding same manner as in Example 1.

2. Describe the finite field $GF(2^4)$ using polynomial $p(x) = x^{16} - x$. What are the irreducible factors of $p(x)$? Based on these irreducible factors find the finite fields that are isomorphic to $GF(2^4)$.

**Answer:** The polynomial $p(x) = x^{16} - x$ has 16 distinct roots since $p(x) = x^{16} - x$ and $p'(x) = -1$ have no common factors of positive degree. The finite field $GF(2^4)$ consists of these sixteen roots of the polynomial $p(x)$.

The polynomial $p(x) = x^{16} - x$ is not irreducible in $\mathbb{Z}_2[x]$. In fact using maple command “Factor(x^16 - x) mod 2;” we see that

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

We can check using maple command “Irreduc(x^4 + x^3 + x^2 + x + 1) mod 2;” that the factor $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$. Similarly the factors $x^4 + x + 1$ and $x^4 + x^3 + 1$ can be verified to be irreducible in $\mathbb{Z}_2[x]$.

Each of the irreducible factor gives rise to a finite field with $2^4$ elements. Hence we have the following additional finite fields $\mathbb{Z}_2[x]/<x^4 + x + 1>$, $\mathbb{Z}_2[x]/<x^4 + x^3 + 1>$ and $\mathbb{Z}_2[x]/<x^4 + x^3 + x^2 + x + 1>$. However each one is isomorphic to $GF(2^4)$. 

---

**Direction:** *This homework is due on April 20, 2006. In order to receive full credit, answer each problem completely and must show all work.*
3. Construct a field of order 27 and carry out the analysis done in Example 1 (on page 383), including the conversion table.

**Answer:** To construct a finite field of order 27, we start with an irreducible polynomial $p(x)$ of degree 3 in $\mathbb{Z}_3[x]$. An irreducible polynomial in $\mathbb{Z}_3[x]$ is $p(x) = x^3 + 2x + 1$. Hence $GF(3^3)$ will be isomorphic to the field $\mathbb{Z}_3[x]/<x^3 + 2x + 1>$. The conversion table can be constructed using the following maple commands:

```maple
> f := x -> x^3 + 2x + 1:
> for i from 1 to 26 do
> temp := Powmod(x, i, f(x), x) mod 3:
> print(x^i, ' field element ', temp);
> od:
```

4. Draw the subfield lattice of $GF(3^{18})$ and of $GF(3^{30})$.

**Answer:** The subfield lattice of $GF(3^{18})$ and of $GF(3^{30})$ are shown below.
5. How does the subfield lattice of $GF(2^{30})$ compare with the subfield lattice of $GF(3^{30})$?

**Answer:** The subfield lattice of $GF(3^{30})$ is given by

If we replace the base 3 by 2 in the above diagram, then we have a lattice diagram for the subfields of the field $GF(2^{30})$. Hence the lattice diagrams are identical to each other.

6. Let $E$ be the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$, where $p$ is a prime and $n$ is a positive integer. Show that set of zeros

$$S = \{ \alpha \in E \mid f(\alpha) = 0 \}$$

is closed under addition, subtraction, multiplication and division (by nonzero elements).

**Answer:** Let $S = \{ \alpha \in E \mid f(\alpha) = 0 \}$. Hence $S = \{ \alpha \in E \mid \alpha^{p^n} = \alpha \}$. Let $\alpha, \beta \in S$. Hence we have $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$. We want to show that $\alpha + \beta \in S$. Since characteristic of $E$ is $p$, therefore $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$. Hence $\alpha + \beta \in S$.

If $p$ is an odd prime, then $(\alpha - \beta)^{p^n} = \alpha^{p^n} + (-\beta)^{p^n} = \alpha^{p^n} - \beta^{p^n} = \alpha - \beta$, and $\alpha - \beta \in S$. If $p$ is an even prime, that is, $p = 2$, then each element of $E$ are additive inverse of itself (because $2\alpha = 0$ implies $\alpha = -\alpha$). Therefore in this case $(\alpha - \beta)^{2^n} = \alpha^{2^n} + (-\beta)^{2^n} = \alpha^{2^n} + (-\beta)(\beta^{2^{n-1}} = \alpha^{2^n} - \beta^{2^n} = \alpha - \beta$, and $\alpha - \beta \in S$. Hence the set $S$ is closed under subtraction.

Since $(\alpha\beta)^{p^n} = \alpha^{p^n} \beta^{p^n} = \alpha \beta$ and $(\alpha\beta^{-1})^{p^n} = \alpha^{p^n} (\beta^{-1})^{p^n} = \alpha^{p^n} (\beta^{p^n})^{-1} = \alpha \beta^{-1}$, therefore $S$ is closed under multiplication and division.
7. Prove that for each prime \( p \) and each positive integer \( n \) there is, upto isomorphism, a unique finite field of order \( p^n \). (Hint: see Theorem 22.1 on page 382.)

**Answer:** We want to show that \( E \) is unique up to isomorphism. That is if \( K \) is any other finite field of order \( p^n \), then \( E \cong K \). The characteristic of \( K \) is \( p \). By Corollary 3 (page 284), \( K \) contains a subfield isomorphic to \( \mathbb{Z}_p \). Since \( K \) is a field of order \( p^n \), the nonzero elements form a group under multiplication of order \( p^n - 1 \). By Lagrange's Theorem, if \( a \) is a nonzero element of \( K \), then \( a^{p^n - 1} = 1 \) for all nonzero \( a \in K \). Hence \( f(a) = a^{p^n} - a = a(a^{p^n - 1} - 1) = 0 \). Therefore if \( a \in K \) is a nonzero element, then \( a \) is a zero of \( f(x) \). Therefore \( K \) must be splitting field of \( f(x) \) over \( \mathbb{Z}_p \). Since \( E \) and \( K \) are two splitting fields of \( f(x) \) over \( \mathbb{Z}_p \), by Lemma 2, we have \( K \cong E \). Hence \( E \) is unique up to isomorphism.