Solution to Problem 29: i) Let $L = \mathbb{F}_2[x]/ < x^3 + x + 1 >$. Recall that if $\overline{x}$ is the coset $x + < x^3 + x + 1 >$ then every element of L can be uniquely expressed as $a + b\overline{x} + c\overline{x}^2$ for some $a, b, c \in \mathbb{F}_2$. We have two choices for each a, b, c so we get $2^3 = 8$ elements in L.

ii) Explicitely, the non-zero elelemts of L are

$$1,\ \overline{x},\ 1+\overline{x},\ \overline{x}^2,\ 1+\overline{x}^2,\ x+\overline{x}^2,\ 1+x+\overline{x}^2.$$

Note that in $\mathbb{F}_2$ we have $1 = -1$ and in L we have $\overline{x}^3 + \overline{x} + 1 = 0$. It follows that $\overline{x}^3 = 1 + \overline{x}$ and $\overline{x}^4 = \overline{x} + \overline{x}^2$. Note now that

$$\overline{x}(1 + \overline{x}^2) = \overline{x} + \overline{x}^3 = 1,$$

$$(1 + \overline{x})(\overline{x} + \overline{x}^2) = \overline{x} + \overline{x}^3 = 1,$$

$$\overline{x}^2(1 + \overline{x} + \overline{x}^2) = \overline{x}^2 + \overline{x}^3 + \overline{x}^4 = \overline{x}^2 + (1 + \overline{x}) + (\overline{x} + \overline{x}^2) = 1.$$

It follows that

$$1 \cdot \overline{x} \cdot (1 + \overline{x}) \cdot \overline{x}^2 \cdot (1 + \overline{x}^2) \cdot (x + \overline{x}^2) \cdot (1 + x + \overline{x}^2) =$$

$$= [\overline{x}(1 + \overline{x}^2)][(1 + \overline{x})(\overline{x} + \overline{x}^2)][\overline{x}^2(1 + \overline{x} + \overline{x}^2)] = 1 = -1.$$

Remark. The conlusion of the problem can be reached in a more theoretical way. Consider a finite field F. Every non-zero element $x \in F$ has its inverse x^{-1}. Note that $x = x^{-1}$ iff $x^2 - 1 = 0$, iff $x = 1$ or $x = -1$. It follows that all non-zero elements of F different from 1 and -1 can be divided into pairs of reciprocal elements. The product of elements in each pair is 1, so the product of all elements in F different from $0, 1, -1$ equals 1. It follows that if F has characteristic 2 then the product of all non-zero elements of F is 1 (which is the same as -1), and if the characteristic of F is odd (so $1 \neq -1$), the product of all non-zero elements is -1.

Solution to Problem 36 Recall that the only irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$ is $x^2 + x + 1$. Suppose that $f \in \mathbb{F}_2[x]$ has degree 4, has no roots in $\mathbb{F}_2$ and is not irreducible. Then it does not have any irreducible factors of degree 1, so it must be a product of two irreducible polynomials of degree 2. Since $x^2 + x + 1$ is the only irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$, we must have $f = (x^2 + x + 1)^2 =$

$x^4 + x^2 + 1$. We proved that a degree 4 polynomial in $\mathbb{F}_2[x]$ is irreducible iff it does not have a root in $\mathbb{F}_2$ and is not equal to $x^4 + x^2 + 1$. Now we have 16 degree 4 polynomials in $\mathbb{F}_2[x]$. The ones which do not have a root end with 1 and have odd number of non-zero terms. Thus they must have three non-zero termsi or five non-zero terms. Consequently, the irreducible polynomials of degree 4 are:

$$x^4 + x^3 + 1, \quad x^4 + x + 1, \quad x^4 + x^3 + x^2 + x + 1.$$