MAT 312/AMS 351: Applied Algebra
Solutions to Problem Set 11 (22pts)

Problem I (4pts)

Let F be a field and $p \in F[x]$ be a polynomial of positive degree. Show that the ring $F[x]/(p)$ of polynomial congruence classes of p is a field if and only if p is irreducible.
Note: It is shown on p280 that $F[x]/(p)$ is a ring, even if F is just a ring; do not check this again.

Suppose p is reducible, i.e. $p = qr$ for some polynomials $q, r \in F[x]$ of positive degrees. Since the degrees of these polynomials are less than the degree of p (which is the sum of the degrees of q and r), p does not divide q, r in $F[x]$ and

$$[q]_p, [r]_p \neq [\mathbf{0}]_p \in F[x]/(p).$$

However,

$$[q]_p \cdot [r]_p = [qr]_p = [p]_p = [\mathbf{0}]_p \in F[x]/(p).$$

Thus, $[q]_p$ and $[r]_p$ are zero divisors in $F[x]/(p)$. Since the ring $F[x]/(p)$ contains zero divisors, it is not a field.

Suppose p is irreducible. By the Division with Remainder for Polynomials, every element of $F[x]/(p)$ is (uniquely) of the form $[q]_p$ with $q \in F[x]$ of degree less than the degree of p. Let $q \neq \mathbf{0}$ be any such polynomial. Since p is irreducible, no polynomial of degree smaller than the degree of p divides p. Since the degree of p is larger than the degree of q, no polynomial of degree at least the degree of p divides q. Thus, the constant polynomial $\mathbf{1} \in F[x]$ is a gcd of p and q and there exist polynomials $s, t \in F[x]$ such that

$$sp + tq = \mathbf{1} \in F[x] \qquad \Longrightarrow \qquad [s]_p[p]_p + [t]_p[q]_p = [\mathbf{1}]_p \in F[x]/(p).$$

Since $[p]_p = [\mathbf{0}]_p$ in $F[x]/(p)$, the last equation says that $[t]_p$ is a multiplicative inverse of $[q]_p$ in $F[x]/(p)$. Thus, every nonzero element of $F[x]/(p)$ has a multiplicative inverse, and so the ring $F[x]/(p)$ is a field.

Problem J (6+3+2pts)

Let F be a field. A polynomial $p\in F[x]$ of positive degree d is called primitive *if the remainders of the monomials x^i, $i=0,1,\ldots$, from dividing by p include every nonzero polynomial of degree less than d. Show that*

(a) *a primitive polynomial p is prime;*

(b) $1+x+x^2+x^3+x^4\in\mathbb{Z}_2[x]$ *is prime, but not primitive;*

(c) *the smallest $n\in\mathbb{Z}^+$ such that a primitive degree d polynomial $p\in\mathbb{Z}_2[x]$ divides x^n-1 is 2^d-1.*

(a) Since F is a field, $p\in F[x]$ is prime if and only if p is irreducible. By Problem I, the latter is the case if and only if the ring $F[x]/(p)$ is a field, i.e. every nonzero element of $F[x]/(p)$ has a multiplicative inverse. By the Division with Remainder for Polynomials, every element of $F[x]/(p)$ is (uniquely) of the form $[q]_p$ with $q\in F[x]$ of degree less than the degree of p. If p is primitive, then every element of $F[x]/(p)$ equals $[x^i]_p=[x]_p^i$ for some $i\in\mathbb{Z}^{\ge 0}$ (not necessarily unique). It is thus sufficient to show that for every $i\in\mathbb{Z}^{\ge 0}$ such that p does not divide x^i there exist

$$j\in\mathbb{Z}^{\ge 0} \quad\text{and}\quad u\in F-\{0\} \qquad \text{s.t.} \qquad [x^i]_p\cdot[x^j]_p\equiv\big[x^{i+j}\big]_p=[\mathbf{u}]_p\in F[x]/(p),$$

where $\mathbf{u}\in F[x]$ is the constant polynomial with value u; this would imply that $[u^{-1}x^j]_p$ is a multiplicative inverse of $[x^i]_p$.

We first show that $F[x]/(p)$ has no zero divisors. Suppose

$$i,j\in\mathbb{Z}^{\ge 0} \qquad\text{and}\qquad [x^i]_p\cdot[x^j]_p=[\mathbf{0}]_p\in F[x]/(p)\,.$$

The last statement implies that p divides x^{i+j} in $F[x]$ and thus $p=x^d$ for some $d\in\mathbb{Z}^+$ such that $d\le i+j$. The only nonzero remainders of the monomials x^i with $i\in\mathbb{Z}^{\ge 0}$ from dividing by p are then x^i with $i=0,1,\ldots,d-1$. These are all the nonzero monomials of degree less than d if and only if $d=1$ and $F=\mathbb{Z}_2$. If the latter is the case, either $i\ge d$ or $j\ge d$, and so either $[x^i]_p=[\mathbf{0}]_p$ or $[x^j]_p=[\mathbf{0}]_p$. Whether or not $d=1$ and $F=\mathbb{Z}_2$, we conclude that $F[x]/(p)$ has no zero divisors. Since $p(x)=x$ is an irreducible polynomial, for the remainder of the proof we assume that $p(x)\neq x$ and thus $[x^i]_p\neq[\mathbf{0}]_p$ for all $i\in\mathbb{Z}^{\ge 0}$.

Suppose next that the field F is finite. We then show that the element $[x]_p$ of $F[x]/(p)$ has a finite multiplicative order. Since every element of $F[x]/(p)$ is (uniquely) of the form $[q]_p$ with $q\in F[x]$ of degree less than the degree of p, the ring $F[x]/(p)$ is then finite. Since the set $\mathbb{Z}^{\ge 0}$ is infinite, it follows that there exist

$$i,j\in\mathbb{Z}^{\ge 0}\ \text{s.t.}\ i<j,\ [x^i]_p=[x^j]_p\neq[\mathbf{0}]_p\in F[x]/(p) \quad\Longrightarrow\quad [x^i]_p\big([x^{j-i}]_p-[\mathbf{1}]_p\big)=[\mathbf{0}]_p\in F[x]/(p).$$

Since $F[x]/(p)$ has no zero divisors, the last statement implies that $[x^{j-i}]_p=[\mathbf{1}]_p$. Thus, there exists $N\in\mathbb{Z}^+$ so that $[x^N]_p=[\mathbf{1}]_p$.

If $[x^i]_p$ is any nonzero element of $F[x]/(p)$ and $j\in\mathbb{Z}^{\ge 0}$ is such that $i+j$ is divisible by N, then

$$[x^i]_p\cdot[x^j]_p=[x]_p^{i+j}=[\mathbf{1}]_p\in F[x]/(p).$$

Thus, $[x^j]_p$ is a multiplicative inverse of $[x^i]_p$. We conclude that every nonzero element of $F[x]/(p)$ has a multiplicative inverse and thus $F[x]/(p)$ is a field.

Suppose now that F is infinite and $[x^i]_p$ with $i\in\mathbb{Z}^{\ge 0}$ is any nonzero element of $F[x]/(p)$. Since $F-\{0\}$ is infinite, there exist

$$j\in\mathbb{Z},\ u\in F-\{0\} \qquad \text{s.t.} \qquad j\ge i,\quad [x^j]_p=[\mathbf{u}]_p\in F[x]/(p).$$

This implies $[x^i]_p\cdot[x^{j-i}]_p=[\mathbf{u}]_p$ and so $[x^i]_p$ is a unit in $F[x]/(p)$. We conclude that every nonzero element of $F[x]/(p)$ has a multiplicative inverse and thus $F[x]/(p)$ is a field.

Note. The reasoning in the previous paragraph in fact implies that F cannot be infinite if $F[x]$ contains a primitive polynomial p.

(b) Since $x=0,1$ are not roots of $1+x+x^2+x^3+x^4$ over $\mathbb{Z}_2$, this polynomial has no linear factors in $\mathbb{Z}_2[x]$. If it is not prime/irreducible, then it is a product of two (not necessarily distinct) irreducible degree 2 polynomials. An irreducible degree 2 polynomial over $\mathbb{Z}_2$ must contain the constant term 1 (o/w it would be divisible by x) and an odd number of terms overall (o/w $x=1$ would be a root and $(x-1)$ would divide this polynomial). The only such degree 2 polynomial is $1+x+x^2$. Since

$$\big(1+x+x^2\big)^2=1+x^2+x^4\in\mathbb{Z}_2[x],$$

it follows that $1+x+x^2+x^3+x^4$ has no degree 2 factors either and is thus irreducible/prime in $\mathbb{Z}_2[x]$.

The remainders of the monomials x^i, $i=0,1,\ldots$, from dividing by $1+x+x^2+x^3+x^4$ are

$$1,x,x^2,x^3,x^4=1+x+x^2+x^3,x^5=x\big(1+x+x^2+x^3\big)=\big(x+x^2+x^3\big)+\big(1+x+x^2+x^3\big)=1,\ldots;$$

the remainders cycle afterwards. Thus, the remainders consist of only 5 out of the 2^4-1 polynomials of degree less than 4, and so $1+x+x^2+x^3+x^4$ is not a primitive polynomial.

(c) By (a) and Problem I, $\mathbb{Z}_2[x]/(p)$ is a field. Thus, the group G_p of units in $\mathbb{Z}_2[x]/(p)$ consists of all nonzero elements. Since every element of $\mathbb{Z}_2[x]/(p)$ is (uniquely) of the form $[q]_p$ with $q\in\mathbb{Z}_2[x]$ of degree less than the degree d of p, it follows that $|G_p|=2^d-1$. Since $[x]_p$ generates the multiplicative group G_p, the order of this element, i.e. the smallest $n\in\mathbb{Z}^+$ such that

$$[x]_p^n=[\mathbf{1}]_p\in G_p\subset\mathbb{Z}_2[x]/(p)$$

is $|G_p|$. The last equality is equivalent to p dividing x^n-1 in $\mathbb{Z}_2[x]$.

Problem K (3+1+3pts)

Let $f:\mathbb{Z}_2^4 \longrightarrow \mathbb{Z}_2^7$ be the cyclic code generated by the polynomial $p(x)=1+x+x^3$.

(a) *Show that this code corrects one error.*

(b) *Find the parity polynomial $q(x)$ for $p(x)$.*

(c) *The message received, possibly with an error, is 0110110. What message (codeword) was sent? What word does this codeword stand for?*

(a) The codewords of this code are the polynomials $pa\in\mathbb{Z}_2[x]$ with $a\in\mathbb{Z}_2[x]$ being a polynomial of degree less than 4. An error in the i-th bit, with $i=1,2,\ldots,7$, is an extra x^{i-1} added to a codeword $pa\in\mathbb{Z}_2[x]$. The remainders of these monomials from dividing by p are

$$1, \quad x, \quad x^2, \quad x^3=1+x, \quad x^4=x(1+x)=x+x^2,$$
$$x^5=x(x+x^2)=x^2+(1+x)=1+x+x^2, \quad x^6=x(1+x+x^2)=(x+x^2)+(1+x)=1+x^2.$$

Since they are all distinct, this code can determine in which bit i a single error occurred from the remainders of dividing by p. Thus, this code corrects one error.

Alternatively, one can show that the minimum length of a nonzero code word is 3. This can done by computing all 2^4-1 nonzero codewords:

$$1 \longrightarrow 1+x+x^3, \quad x \longrightarrow x+x^2+x^4, \quad x^2 \longrightarrow x^2+x^3+x^5, \quad x^3 \longrightarrow x^3+x^4+x^6,$$
$$1+x \longrightarrow 1+x^2+x^3+x^4, \quad 1+x^2 \longrightarrow 1+x+x^2+x^5, \quad 1+x^3 \longrightarrow 1+x+x^4+x^6,$$
$$x+x^2 \longrightarrow x+x^3+x^4+x^5, \quad x+x^3 \longrightarrow x+x^2+x^3+x^6, \quad x^2+x^3 \longrightarrow x^2+x^4+x^5+x^6,$$
$$1+x+x^2 \longrightarrow 1+x^4+x^5, \quad 1+x+x^3 \longrightarrow 1+x^2+x^6, \quad 1+x^2+x^3 \longrightarrow 1+x+x^2+x^3+x^4+x^5+x^6,$$
$$x+x^2+x^3 \longrightarrow x+x^5+x^6, \quad 1+x+x^2+x^3 \longrightarrow 1+x^3+x^5+x^6.$$

Since the code is linear, the codewords after the first row are obtained from the already computed codewords by adding the appropriate elements from the first row.

(b) Since

$$x^7-1=(x-1)\big(x^6+x^5+x^4+x^3+x^2+x+1\big)=(x-1)\big(x^3+x^2+1\big)\big(x^3+x+1\big),$$

the parity polynomial $q(x)$ for $p(x)=(1+x+x^3)$ is

$$q(x)=(1+x)\big(1+x^2+x^3\big)=1+x+x^2+x^4\,.$$

(c) This message corresponds to the polynomial $b(x)=x+x^2+x^4+x^5$. Dividing it with remainder by $p(x)$, we obtain

$$\begin{aligned} x^5+x^4+x^2+x = x^2\big(x^3+x+1\big)+\big(x^4+x^3+x\big) &= \big(x^2+x\big)\big(x^3+x+1\big)+\big(x^3+x^2\big) \\ &= \big(x^2+x+1\big)\big(x^3+x+1\big)+\big(x^2+x+1\big). \end{aligned}$$

By part (a), the remainder $1+x+x^2$ arises from x^5. The relevant codeword is thus

$$b(x)+x^5=x+x^2+x^4.$$

This codeword arises from the polynomial x, which corresponds to the word 0100 (before encoding).