Abstract Algebra Homework 11

Joe Loser

April 30, 2016

This problem set includes problems $3c, 4b, 24$, and an extra problem from section 17.4.

3) Use the division algorithm to find $q(x)$ and $r(x)$ such that $a(x) = q(x)b(x) + r(x)$ with $\deg r(x) < \deg b(x)$.

3c) $a(x) = 4x^5 - x^3 + x^2 + 4$ and $b(x) = x^3 - 2$ where $a(x), b(x) \in \mathbb{Z}_5[x]$.

<u>Solution</u>: First note that in $\mathbb{Z}_5[x], a(x) \equiv 4x^5 + 4x^3 + x^2 + 4$ and $b(x) \equiv x^3 + 3$.

Now performing long division, we have

$$\begin{array}{r|l} & \ 4x^2 \quad +4 \\ \hline x^3+3 & 4x^5 + 4x^3 \quad + x^2 \quad + 4 \\ & -4x^5 \qquad -12x^2 \\ \cline{2-2} & \qquad 4x^3 - 11x^2 \quad + 4 \\ & \qquad -4x^3 \qquad\quad -12 \\ \cline{2-2} & \qquad\qquad -11x^2 \quad -8 \end{array}$$

Thus,

$$\begin{aligned} a(x) &= (4x^2 + 4) \cdot (x^3 + 3) + (-11x^2 - 8) \\ &\equiv (4x^2 + 4) \cdot (x^3 + 3) + (4x^2 + 2). \end{aligned}$$

$\square$

4) Find the greatest common divisor of each of the following pairs $p(x)$ and $q(x)$ of polynomials. If $d(x) = \gcd(p(x), q(x))$, find two polynomials $a(x)$ and $b(x)$ such that $d(x) = a(x)p(x) + b(x)q(x)$.

4b) $p(x) = x^3 + x^2 - x + 1$ and $q(x) = x^3 + x - 1$ where $p(x), q(x) \in \mathbb{Z}_2[x]$.

First note that $\mathbb{Z}_2[x]$, $p(x) \equiv x^3 + x^2 + x + 1$ and $q(x) \equiv x^3 + x + 1$.

Performing the first stage of long division, we have that

$$\begin{array}{r|l} & \qquad\qquad\quad 1 \\ \hline x^3+x^2+x+1 & x^3 \qquad + x + 1 \\ & -x^3 - x^2 - x - 1 \\ \cline{2-2} & \qquad -x^2 \end{array}$$

Note that in $\mathbb{Z}_2[x], -x^2 \equiv x^2$ and $2x^2 \equiv 0$. So

$$x^3 + x + 1 = 1 \cdot (x^3 + x^2 + x + 1) + (x^2). \tag{1}$$

In the second stage of long division, we get

$$\begin{array}{r|l} & \qquad\qquad x + 1 \\ \hline x^2 & x^3 + x^2 + x + 1 \\ & -x^3 \\ \cline{2-2} & \qquad x^2 \\ & \quad -x^2 \\ \cline{2-2} \end{array}$$

So we have that

$$x^3 + x^2 + x + 1 = (x+1) \cdot (x^2) + (x+1). \tag{2}$$

In the third stage, we get

$$\begin{array}{r|l} & \quad\; x-1 \\ \hline x+1 & x^2 \\ & -x^2 - x \\ \hline & \quad -x \\ & \quad\;\; x+1 \\ \hline & \qquad\;\; 1 \end{array}$$

Then

$$x^2 = (x+1) \cdot (x+1) + (1). \tag{3}$$

In the last stage of long division, we have

$$\begin{array}{r|l} & x+1 \\ \hline 1 & x+1 \\ & -x \\ \hline & \quad 1 \\ & \; -1 \\ \hline & \quad 0 \end{array}$$

So

$$x + 1 = (1) \cdot (x+1) + 0. \tag{4}$$

Thus $\gcd(p(x), q(x)) = 1$. Performing the back substitution, we have the following

$$\begin{aligned}
1 &= x^2 - (x+1)(x+1) \\
&= x^2 - (x+1)[(x^3 + x^2 + x + 1) - x^2(x+1)] \\
&= x^2 + (x+1)(x^3 + x^2 + x + 1) + x^2(x+1)^2 \\
&= x^2\Big(1 + (x+1)^2\Big) + (x+1)(x^3 + x^2 + x + 1) \\
&= [x^3 + x + 1 + (x^3 + x^2 + x + 1)](x^2) + (x+1)(x^3 + x^2 + x + 1) \\
&= (x^3 + x^2 + x + 1)(x^2 + x + 1) + (x^2)(x^3 + x + 1).
\end{aligned}$$

Thus

$$\begin{aligned}
1 &= (x^2 + x + 1)(x^3 + x^2 + x + 1) + (x^2)(x^3 + x + 1) \\
&= a(x)p(x) + b(x)q(x).
\end{aligned}$$

To check this holds in $\mathbb{Z}_2[x]$, we multiply everything out. We get that

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

$\square$

24) Show that $x^p - x$ has p distinct zeros in $\mathbb{Z}_p$ for any prime p. Conclude that

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1)).$$

Proof: By Fermat's Little Theorem, for all $a \in \mathbb{Z}_p$ we have that $a^p = a$. So $a^p - a = 0$. Thus every $a \in \mathbb{Z}_p$ is a zero of the polynomial $x^p - x$. Note that the polynomial has degree p and p zeros in $\mathbb{Z}_p$. The numbers $0, 1, \cdots, p-1$ are the roots of the equation $x^p - x$, i.e. the p distinct roots. Hence it must split into p distinct linear factors in $\mathbb{Z}_p[x]$ as follows:

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1)).$$

□

E1) Construct a field with 8 elements.

Solution: Since $8 = 2^3$ we start with a field $\mathbb{Z}_2$ of characteristic 2 and look for an irreducible polynomial of degree 3 in $\mathbb{Z}_2[x]$. Such a polynomial is $p(x) = x^3 + x + 1$.

We will show that

$$K := \frac{\mathbb{Z}_2[x]}{\langle x^3 + x + 1\rangle}$$

is a field of 8 elements.

To see why $p(x)$ is irreducible in $\mathbb{Z}_2[x]$, since it of degree 3 or lower, we can look at all of the roots in $\mathbb{Z}_2$ since $g(x)$ is irreducible if and only if p does not have a root, i.e. $p(a) \neq 0$ for all $a \in \mathbb{Z}_2$. We have that $g(0) = 1$ and $g(1) = 3 \equiv 1$. So neither 0 or 1 are a root of $p(x)$. Hence we see that we $p(x)$ is irreducible over $\mathbb{Z}_2[x]$.

By the Division Algorithm, we have that

$$p(x) + \langle x^3 + x + 1\rangle = a_0 + a_1 x + a_2 x^2 + \langle x^3 + x + 1\rangle$$

where $a_0, a_1, a_2 \in \mathbb{Z}_2$. So

$$K = \{a_0 + a_1 x + a_2 x^2 + \langle x^3 + x + 1\rangle \,|\, a_0, a_1, a_2 \in \mathbb{Z}_2\}.$$

Note that since $a_0, a_1, a_2 \in \mathbb{Z}_2$ we see that the order of K which we denote $|K|$ is

$$\begin{aligned} |K| &\leq |\mathbb{Z}_2| \times |\mathbb{Z}_2| \times |\mathbb{Z}_2| \\ &= 2 \times 2 \times 2 \\ &= 8. \end{aligned}$$

To see why K has exactly 8 elements, suppose $a_0 + a_1 x + a_2 x^2 + \langle x^3 + x + 1\rangle = b_0 + b_1 x + b_2 x^2 + \langle x^3 + x + 1\rangle$. Then

$$(a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2 \in |x^3 + x + 1|.$$

That is,

$$\underbrace{x^3 + x + 1}_{\deg 3} \mid \underbrace{(a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2}_{\deg<3}.$$

So $(a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2 = 0$. Hence $a_0 = b_0, a_1 = b_1$ and $a_2 = b_2$. Therefore $|K| = 8$.

To explicitly see what the elements of K are, let $\alpha := x + \langle x^3 + x + 1\rangle \in K$. Now we want to compute the powers of α for $i = 1 \cdots 7$. This will give us the elements of K.

$$\begin{aligned} \alpha^2 &= (x + \langle x^3 + x + 1\rangle)^2 \\ &= x^2 + 2x\langle x^3 + x + 1\rangle + (\langle x^3 + x + 1\rangle)^2 \\ &\equiv x^2 + \langle x^3 + x + 1\rangle. \end{aligned}$$

In K, $x^3 + x + 1 = 0 \iff \alpha^3 + \alpha + 1 = 0 \iff \alpha^3 = \alpha + 1$. That is, $\alpha^3 = x + 1 + \langle x^3 + x + 1\rangle$. Next we see that

$$\begin{aligned} \alpha^4 &= \alpha^3 \cdot \alpha \\ &= (\alpha + 1) \cdot \alpha \\ &= (x + 1) \cdot x \\ &\equiv x^2 + x + \langle x^3 + x + 1\rangle. \end{aligned}$$

Also

$$
\begin{aligned}
\alpha^5 &= \alpha^3 \cdot \alpha^2 \\
&= (\alpha+1) \cdot \alpha^2 \\
&= \alpha^3 + \alpha^2 \\
&= (\alpha+1) + \alpha^2 \\
&\equiv x + 1 + x^2 \\
&\equiv x^2 + x + 1 + \langle x^3 + x + 1 \rangle.
\end{aligned}
$$

Continuing on, we have that

$$
\begin{aligned}
\alpha^6 &= \alpha^3 \cdot \alpha^3 \\
&= (x+1)(x+1) \\
&= x^2 + 2x + 1 \\
&\equiv x^2 + 1 + \langle x^3 + x + 1 \rangle.
\end{aligned}
$$

Lastly we have that

$$
\begin{aligned}
\alpha^7 &= \alpha^4 \cdot \alpha^3 \\
&= (\alpha^2 + \alpha) \cdot (\alpha + 1) \\
&= \alpha^3 + \alpha^2 + \alpha^2 + \alpha \\
&= \alpha^3 + \alpha \\
&= (\alpha + 1) + \alpha \\
&\equiv 1.
\end{aligned}
$$

Explicitly listing the elements of K, we have that

$$
\begin{aligned}
K &= \{0, x, x^2, x+1, x^2+x, x^2+x+1, x^2+1, 1\} \\
&= \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}.
\end{aligned}
$$

$\square$