Abstract Algebra
Day 33 Class Work Solutions

For the problems below, fix $x^2-1 \in \mathbb{Z}_7[x]$ and define $\langle x^2-1\rangle = \{(x^2-1)\cdot q(x) \mid q(x) \in \mathbb{Z}_7[x]\}$. ← i.e., the principal ideal generated by x^2-1.

1. List three elements of $\mathbb{Z}_7[x]$ that are contained in $\langle x^2-1\rangle$.

   Solution. Answers will vary. Elements of $\langle x^2-1\rangle$ have the form $(x^2-1)\cdot q(x)$ where $q(x) \in \mathbb{Z}_7[x]$. Examples: $x^2-1 = (x^2-1)\cdot 1$ and $4x^5+2x^3+x = (x^2-1)\cdot(4x^3+6x)$.

2. Let $f(x) = 4x^5+2x^3+4x+1 \in \mathbb{Z}_7[x]$ and recall that

$$f(x) = (x^2-1)\cdot(4x^3+6x) + (3x+1).$$

← In $\mathbb{Z}_7[x]$, we have $10x+1 = 3x+1$.

   (a) Explain why $f(x)$ is *not* contained in $\langle x^2-1\rangle$.

   Solution. As shown above, $f(x)$ is *not* a multiple of x^2-1, since the remainder $3x+1$ is not zero.

   (b) Using the result of the division algorithm above, find $g(x) \in \mathbb{Z}_7[x]$ of the smallest degree such that $f(x)+\langle x^2-1\rangle = g(x)+\langle x^2-1\rangle$. **Ans:** $g(x) = 3x+1$.

   Solution. Let $g(x) = 3x+1$. Then $f(x)-g(x) = (x^2-1)\cdot(4x^3+6x) \in \langle x^2-1\rangle$. Thus, $f(x)+\langle x^2-1\rangle = g(x)+\langle x^2-1\rangle$.

   (c) In part (b), describe how $f(x)$ and $g(x)$ are related. (**Hint:** Think $f(x)-g(x)$.)

   Solution. Their difference is a multiple of x^2-1, and hence is in $\langle x^2-1\rangle$.

3. Let $f(x) = 2x^9+5x^7+4x^3+3 \in \mathbb{Z}_7[x]$.

   (a) Find $g(x) \in \mathbb{Z}_7[x]$ of the smallest degree such that $f(x)+\langle x^2-1\rangle = g(x)+\langle x^2-1\rangle$. The following Mathematica code should help:

```
In[16]:= f = 2 x^9 + 5 x^7 + 4 x^3 + 3

In[17]:= PolynomialMod[PolynomialQuotientRemainder[f, x^2 - 1, x], 7]
Out[17]= {2 x^7 + 4 x, 4 x + 3}
```

   Solution. The Mathematica output shows that

$$f(x) = (x^2-1)\cdot q(x) + (4x+3),$$

   where $q(x) = 2x^7+4x$. Now let $g(x) = 4x+3$. Then, $f(x)-g(x) = (x^2-1)\cdot q(x) \in \langle x^2-1\rangle$. Thus, $f(x)+\langle x^2-1\rangle = g(x)+\langle x^2-1\rangle$.

   (b) In part (a), describe how $f(x)$ and $g(x)$ are related.

   Solution. Their difference is a multiple of x^2-1, and hence is in $\langle x^2-1\rangle$.

4. (a) Let $f(x) \in \mathbb{Z}_7[x]$. Explain why $f(x)+\langle x^2-1\rangle$ can be "reduced" to $(ax+b)+\langle x^2-1\rangle$ where $a, b \in \mathbb{Z}_7$.

   Solution. By the division algorithm, we have $f(x) = (x^2-1)\cdot q(x) + (ax+b)$ for some $q(x) \in \mathbb{Z}_7[x]$. Note here that the remainder $ax+b$ has smaller degree than the divisor x^2-1. Now let $g(x) = ax+b$. Then $f(x)-g(x) = (x^2-1)\cdot q(x) \in \langle x^2-1\rangle$. Thus, $f(x)+\langle x^2-1\rangle = g(x)+\langle x^2-1\rangle$.

   (b) Describe all distinct elements of $\mathbb{Z}_7[x]/\langle x^2-1\rangle$. How many are there? **Ans:** 49 cosets.

   Solution. We have $\mathbb{Z}_7[x]/\langle x^2-1\rangle = \{(ax+b)+\langle x^2-1\rangle \mid a, b \in \mathbb{Z}_7\}$ so that the quotient ring contains 49 elements (i.e., 7 choices for a and 7 choices for b).

5. (a) In $\mathbb{Z}_7[x]/\langle x^2-1\rangle$, explain why $x^2+\langle x^2-1\rangle = 1+\langle x^2-1\rangle$.

   Hint: $f(x)+\langle x^2-1\rangle = g(x)+\langle x^2-1\rangle$ if and only if... ?

   Solution. We have $x^2+\langle x^2-1\rangle = 1+\langle x^2-1\rangle$, because $x^2-1 \in \langle x^2-1\rangle$.

   (b) Let $f(x) = 4x^5+2x^3+4x+1 \in \mathbb{Z}_7[x]$ again. After completing part (a) above, Elizabeth wrote down the following calculation:

$$\begin{aligned} f(x)+\langle x^2-1\rangle &= (4x^5+2x^3+4x+1)+\langle x^2-1\rangle \\ &= (4\cdot \boldsymbol{x^2}\cdot \boldsymbol{x^2}\cdot x + 2\cdot \boldsymbol{x^2}\cdot x+4x+1)+\langle x^2-1\rangle \\ &= (4\cdot \mathbf{1}\cdot \mathbf{1}\cdot x+2\cdot \mathbf{1}\cdot x+4x+1)+\langle x^2-1\rangle \end{aligned}$$

   Complete her calculation to verify that $f(x)+\langle x^2-1\rangle = (3x+1)+\langle x^2-1\rangle$. ← Compare with Prob. #2. Which do you prefer?

   Solution. We have $4\cdot 1\cdot 1\cdot x+2\cdot 1\cdot x+4x+1 = 10x+1 = 3x+1$. Thus, $f(x)+\langle x^2-1\rangle = (3x+1)+\langle x^2-1\rangle$.

   (c) Anita says, "I see what she did in part (b). When dealing with coset representatives, we can treat x^2 and 1 to be the same." What might Anita mean?

   Solution. As shown in part (a), we have $x^2+\langle x^2-1\rangle = 1+\langle x^2-1\rangle$. Therefore, *as coset representatives*, we can treat x^2 and 1 to be the same. (But x^2 and -1 are not the same as polynomials in $\mathbb{Z}_7[x]$.)

   For comparison, suppose we want to reduce $2\cdot 378+5\mathbb{Z}$ in $\mathbb{Z}/5\mathbb{Z}$. Since $378+5\mathbb{Z} = 3+5\mathbb{Z}$, we can rewrite $2\cdot 378+5\mathbb{Z}$ as $2\cdot 3+5\mathbb{Z}$, which equals $1+5\mathbb{Z}$. (But 378 and 3 are not the same as integers in $\mathbb{Z}$.)

   (d) Apply Elizabeth's method to Problem #3. Did you get the same result?

   Solution. We have

$$\begin{aligned} f(x)+\langle x^2-1\rangle &= (2x^9+5x^7+4x^3+3)+\langle x^2-1\rangle \\ &= (2\cdot (\boldsymbol{x^2})^4\cdot x+5\cdot (\boldsymbol{x^2})^3\cdot x+4\cdot \boldsymbol{x^2}\cdot x+3)+\langle x^2-1\rangle \\ &= (2\cdot \mathbf{1}^4\cdot x+5\cdot \mathbf{1}^3\cdot x+4\cdot \mathbf{1}\cdot x+3)+\langle x^2-1\rangle \\ &= (4x+3)+\langle x^2-1\rangle, \end{aligned}$$

   which is what we found earlier.

6. Working on Problem #4, Anita says:

   > "I found 49 cosets of the form $(ax+b)+\langle x^2-1\rangle$. But how do I know for sure that they're all distinct? Why can't, for instance, $(5x+3)+\langle x^2-1\rangle$ and $(3x+6)+\langle x^2-1\rangle$ be equal?"

   How would you respond to her?

   Solution. Suppose for contradiction that $(5x+3)+\langle x^2-1\rangle = (3x+6)+\langle x^2-1\rangle$. Then we'd have $(5x+3)-(3x+6)\in\langle x^2-1\rangle$, i.e., $2x+4\in\langle x^2-1\rangle$. This implies $2x+4$ is a multiple of x^2-1, which is a contradiction. Similar argument can be used to show that any pair of the 49 cosets above are, in fact, distinct.

7. (a) Find a zero divisor in $\mathbb{Z}_7[x]/\langle x^2-1\rangle$. (**Hint:** x^2-1 factors. How does that help?)

   (b) Is $\mathbb{Z}_7[x]/\langle x^2-1\rangle$ a field? Why or why not? **Ans:** No. (Why not?)

   Solution. We have...

$$\begin{aligned}((x+1)+\langle x^2-1\rangle)\cdot((x-1)+\langle x^2-1\rangle) &= (x+1)(x-1)+\langle x^2-1\rangle \\ &= (x^2-1)+\langle x^2-1\rangle \\ &= 0+\langle x^2-1\rangle\end{aligned}$$

   so that $(x+1)+\langle x^2-1\rangle$ and $(x-1)+\langle x^2-1\rangle$ are zero divisors, and hence not units. Thus, $\mathbb{Z}_7[x]/\langle x^2-1\rangle$ is *not* a field.

8. Consider the elements $(4x+3)+\langle x^2-1\rangle$ and $(4x+2)+\langle x^2-1\rangle$ in $\mathbb{Z}_7[x]/\langle x^2-1\rangle$. Determine if each is a unit or a zero divisor. Explain how you know.

   Hint: Compute $((4x+3)+\langle x^2-1\rangle)\cdot((ax+b)+\langle x^2-1\rangle)$. How can it be reduced?

   Solution. We compute the following product in $\mathbb{Z}_7[x]/\langle x^2-1\rangle$:

$$\begin{aligned}((4x+3)+\langle x^2-1\rangle)\cdot((ax+b)+\langle x^2-1\rangle) &= (4x+3)\cdot(ax+b)+\langle x^2-1\rangle \\ &= (4a\cdot \boldsymbol{x^2}+(4b+3a)x+3b)+\langle x^2-1\rangle \\ &= (4a\cdot \mathbf{1}+(4b+3a)x+3b)+\langle x^2-1\rangle \\ &= ((4b+3a)x+(4a+3b))+\langle x^2-1\rangle\end{aligned}$$

   This product must equal either $1+\langle x^2-1\rangle$ or $0+\langle x^2-1\rangle$. In either case, the coefficient of x must be zero, i.e., $4b+3a=0$. Solving this equation in $\mathbb{Z}_7$ gives $a=b$, which implies that $4a+3b=7a=0$. Thus, setting $a=b=1$ (or $a=b=2$, 3, 4, 5, or 6), we obtain

$$((4x+3)+\langle x^2-1\rangle)\cdot((x+1)+\langle x^2-1\rangle)=0+\langle x^2-1\rangle,$$

   so that $(4x+3)+\langle x^2-1\rangle$ is a zero divisor.

   Next consider the product

$$\begin{aligned}((4x+2)+\langle x^2-1\rangle)\cdot((ax+b)+\langle x^2-1\rangle) &= (4x+2)\cdot(ax+b)+\langle x^2-1\rangle \\ &= (4a\cdot \boldsymbol{x^2}+(4b+2a)x+2b)+\langle x^2-1\rangle \\ &= (4a\cdot \mathbf{1}+(4b+2a)x+2b)+\langle x^2-1\rangle \\ &= ((4b+2a)x+(4a+2b))+\langle x^2-1\rangle\end{aligned}$$

   As before, set the coefficient of x to be zero, i.e., $2a+4b=0$ in $\mathbb{Z}_7$. This implies that $a=5b$; then substitute that into $4a+2b=1$ to obtain $b=1$ and $a=5$. Thus, we obtain

$$((4x+2)+\langle x^2-1\rangle)\cdot((5x+1)+\langle x^2-1\rangle)=1+\langle x^2-1\rangle,$$

   so that $(4x+2)+\langle x^2-1\rangle$ is a unit, with multiplicative inverse $(5x+1)+\langle x^2-1\rangle$.

---

9. Explore the quotient ring $\mathbb{Z}_7[x]/\langle x^2+1\rangle$, where $\langle x^2+1\rangle=\{(x^2+1)\cdot q(x)\mid q(x)\in\mathbb{Z}_7[x]\}$.

   (a) Describe all distinct elements of $\mathbb{Z}_7[x]/\langle x^2+1\rangle$. How many are there?

   (b) Consider the elements $(4x+3)+\langle x^2+1\rangle$ and $(4x+2)+\langle x^2+1\rangle$ in $\mathbb{Z}_7[x]/\langle x^2+1\rangle$. Determine if each is a unit or a zero divisor. Explain how you know.

   (c) Either find a zero divisor in $\mathbb{Z}_7[x]/\langle x^2+1\rangle$ or explain why one doesn't exist.