Mathematics 351 – Abstract Algebra 1
Solutions for Problem Set 5
October 11, 2007

Section 5.1

3. The congruence classes in $\mathbb{Z}_2[x]/(x^3+x+1)$ are in 1-1 correspondence with the remainders on division by x^3+x+1 in $\mathbb{Z}_2[x]$. These are all the polynomials of degree 2 or less: ax^2+bx+c, with $a,b,c \in \mathbb{Z}_2$. This gives $2 \cdot 2 \cdot 2 = 8$ classes in all:

$$[0],[1],[x],[x+1],[x^2],[x^2+1],[x^2+x],[x^2+x+1].$$

4. This is similar to problem 3 above, except that now the coefficients in the remainders ax^2+bx+c are in $\mathbb{Z}_3$. There are 3 choices for each of a,b,c, so there are $3 \cdot 3 \cdot 3 = 27$ congruence classes in all.

5. The congruence classes in $\mathbb{Q}[x]/(x^2-2)$ are in 1-1 correspondence with the remainders on division by x^2-2 in $\mathbb{Q}[x]$. These are all the polynomials of degree 1 or less: $ax+b$ with $a,b \in \mathbb{Q}$. Since the set $\mathbb{Q}$ is infinite and distinct linear polynomials give distinct congruence classes (that is, $ax+b \equiv cx+d \bmod x^2-2$ only when $a=c$ and $b=d$), there are infinitely many distinct congruence classes in this case.

7. If $p(x)$ has degree k in $\mathbb{Z}_p[x]$, the congruence classes mod $p(x)$ are in 1-1 correspondence with the remainders on division by $p(x)$. These are all polynomials of degree $< k$ and 0:

$$r(x) = a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$$

with $a_i \in \mathbb{Z}_p$ for $i = 0, \ldots, k-1$. This gives p^k different elements since there are p choices for each of the a_i.

8. The statement is true and here is a proof: Since $p(x)$ is relatively prime to $k(x)$, there exist polynomials $u(x)$ and $v(x)$ such that $u(x)p(x)+v(x)k(x)=1$, and as a result, $v(x)k(x) \equiv 1 \bmod p(x)$. Therefore, if $f(x)k(x) \equiv g(x)k(x) \bmod p(x)$, then using Theorem 5.2 part 2, $v(x)f(x)k(x) \equiv v(x)g(x)k(x) \bmod p(x)$, and hence by commutativity and associativity of multiplication,

$$f(x)(v(x)k(x)) \equiv f(x) \cdot 1 \equiv g(x) \cdot 1 \equiv g(x)(v(x)k(x)) \bmod p(x).$$

This shows $f(x) \equiv g(x) \bmod p(x)$.

Section 5.2

1. The tables for $R = \mathbb{Z}_2[x]/(x^3 + x + 1)$ ([,] omitted for simplicity of typing and reading). The addition table:

$+_R$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

The multiplication table:

$+_R$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

By examining the multiplication table, we see that every nonzero element of this congruence class ring does have a multiplicative inverse. Hence R is a field.

3. The tables for $R = \mathbb{Z}_2[x]/(x^2+1)$ ([,] omitted for simplicity of typing and reading). The addition table:

$+_R$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

The multiplication table:

$\cdot_R$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	$x+1$	0

By examining the multiplication table, we see that $x+1$ is a zero-divisor in this ring R. Hence R is not a field.

6. The addition is $[ax+b]+[cx+d] = [(a+c)x+(b+d)]$. The multiplication is done by multiplying $(ax+b)(cx+d) = acx^2 + (bc+ad)x + bd$, then taking the remainder on division by x^2-2, which is $(bc+ad)x + bd + 2ac$. Hence $[ax+b][cx+d] = [(bc+ad)x + bd + 2ac]$.

14. One general method for these is to use the criterion from Theorem 5.9: $[f(x)]$ is a unit in $F[x]/(p(x))$ when $(f(x), p(x)) = 1$ (gcd). You can find the inverse using the Euclidean algorithm

as you learned in Algebraic Structures. An alternate method (simpler) is to solve directly for the coefficients in the multiplicative inverse as follows.

a $[2x-3][ax+b] = [(-3a+2b)x+(4a-3b)]$ by Exercise 6 above. This equals $[1]$ if $-3a+2b=0$ and $4a-3b=1$. Solving simultaneously, we obtain $a=-2$, $b=-3$. So $[2x-3]^{-1} = [-2x-3]$.

b In $\mathbb{Z}_3[x]/(x^2+1)$, $[x^2+x+1] = [x]$ (remainder on division by x^2+1). Hence $[x][2x] = [2x^2] = [1]$, so the multiplicative inverse of $[x]$ is $[2x]$.

c In $\mathbb{Z}_2[x]/(x^3+x+1)$, $[x^2+x+1][x^2] = [1]$ (see multiplication table in answer to question 1 above. Hence $[x^2+x+1]^{-1} = [x^2]$.

Section 5.3

1. We will use the criterion from Theorem 5.10 – to show $F[x]/(p(x))$ is a field, it is equivalent to show $p(x)$ is irreducible in $F[x]$. For polynomials of degree 3 or less, we know that reducibility is equivalent to the polynomial having a root in F.

a Let $f(x) = x^3+2x^2+x+1 \in \mathbb{Z}_3[x]$. We have $f(0)=1$, $f(1)=2$ and $f(2) = 2+2+2+1 = 1$ in $\mathbb{Z}_3$. Hence $f(x)$ has no roots in $\mathbb{Z}_3$ and hence is irreducible in $\mathbb{Z}_3[x]$.

b Similarly, if $g(x) = 2x^3 - 4x^2 + 2x + 1 \in \mathbb{Z}_5[x]$, then $g(2) = 16 - 16 + 4 + 1 \equiv 0 \bmod 5$. Since $g(x)$ has a root in $\mathbb{Z}_5$, so $g(x)$ is not irreducible and the ring $\mathbb{Z}_5[x]/(g(x))$ is *not a field.*

c There are no roots of $h(x) = x^4+x^2+1$ in $\mathbb{Z}_2$. However, it is easy to check that $x^4+x^2+1 = (x^2+x+1)^2$. So $h(x)$ is not irreducible and $\mathbb{Z}_2[x]/(h(x))$ is *not a field.*

2.

a $\mathbb{Q}(\sqrt{2})$ is clearly nonempty ($r, s \in \mathbb{Q}$ are arbitrary). It is also closed under differences since

$$(r+s\sqrt{2}) - (r'+s'\sqrt{2}) = (r-r') + (s-s')\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

It is also closed under products since

$$(r+s\sqrt{2}) \cdot (r'+s'\sqrt{2}) = (rr'+2ss') + (rs'+r's)\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

This shows by Theorem 3.6 that $\mathbb{Q}(\sqrt{2})$ is a subring of $\mathbb{R}$. Since multiplication in $\mathbb{R}$ is commutative, the same is true in the subring. Moreover $1 = 1+0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ so $\mathbb{Q}(\sqrt{2})$ is a commutative ring with identity. Hence the only remaining thing to show to see that it is a field is to show that every nonzero element has a multiplicative inverse in $\mathbb{Q}(\sqrt{2})$. To see this, note that if $r+s\sqrt{2} \neq 0$, then $(r+s\sqrt{2})(r-s\sqrt{2}) = r^2-2s^2$. This cannot be zero, since otherwise, we would have a square root of 2 in $\mathbb{Q}$. Hence

$$(r+s\sqrt{2})^{-1} = \frac{r}{r^2-2s^2} + \left(\frac{-s}{r^2-2s^2}\right)\sqrt{2}$$

is a multiplicative inverse.

b Define

$$\begin{aligned} \varphi : \mathbb{Q}(\sqrt{2}) &\to \mathbb{Q}[x]/(x^2-2) \\ r+s\sqrt{2} &\mapsto [r+sx] \end{aligned}$$

Then φ is clearly 1-1 and onto. Moreover,

$$\begin{aligned} \varphi((r+s\sqrt{2})+(r'+s'\sqrt{2})) &= \varphi((r+r')+(s+s')\sqrt{2}) \\ &= [(r+r')+(s+s')x] \\ &= [r+sx]+[r'+s'x] \\ &= \varphi(r+s\sqrt{2})+\varphi(r'+s'\sqrt{2}). \end{aligned}$$

Moreover,

$$\begin{aligned} \varphi((r+s\sqrt{2})\cdot(r'+s'\sqrt{2})) &= \varphi((rr'+2ss')+(rs'+r's)\sqrt{2}) \\ &= [(rr'+2ss')+(rs'+r's')x] \\ &= [r+sx]\cdot[r'+s'x] \\ &= \varphi(r+s\sqrt{2})\cdot\varphi(r'+s'\sqrt{2}). \end{aligned}$$

This shows that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}[x]/(x^2-2)$ are isomorphic.

5.

a $\mathbb{Q}[\sqrt{3}]$ is clearly nonempty ($r, s \in \mathbb{Q}$ are arbitrary). It is also closed under differences since

$$(r+s\sqrt{3})-(r'+s'\sqrt{3}) = (r-r')+(s-s')\sqrt{3} \in \mathbb{Q}(\sqrt{3}).$$

It is also closed under products since

$$(r+s\sqrt{3})\cdot(r'+s'\sqrt{3}) = (rr'+3ss')+(rs'+r's)\sqrt{3} \in \mathbb{Q}(\sqrt{3}).$$

This shows by Theorem 3.6 that $\mathbb{Q}(\sqrt{3})$ is a subring of $\mathbb{R}$. Since multiplication in $\mathbb{R}$ is commutative, the same is true in the subring. Moreover $1 = 1+0\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ so $\mathbb{Q}(\sqrt{3})$ is a commutative ring with identity. Hence the only remaining thing to show to see that it is a field is to show that every nonzero element has a multiplicative inverse in $\mathbb{Q}(\sqrt{3})$. To see this, note that if $r+s\sqrt{3} \neq 0$, then $(r+s\sqrt{3})(r-s\sqrt{3}) = r^2-3s^2$. This cannot be zero, since otherwise, we would have a square root of 3 in $\mathbb{Q}$. Hence

$$(r+s\sqrt{3})^{-1} = \frac{r}{r^2-3s^2} + \left(\frac{-s}{r^2-3s^2}\right)\sqrt{3}$$

is a multiplicative inverse.

b Define

$$\begin{aligned} \varphi : \mathbb{Q}(\sqrt{3}) &\to \mathbb{Q}[x]/(x^2-3) \\ r+s\sqrt{3} &\mapsto [r+sx] \end{aligned}$$

Then φ is clearly 1-1 and onto. Moreover,

$$\begin{aligned} \varphi((r+s\sqrt{3})+(r'+s'\sqrt{3})) &= \varphi((r+r')+(s+s')\sqrt{3}) \\ &= [(r+r')+(s+s')x] \\ &= [r+sx]+[r'+s'x] \\ &= \varphi(r+s\sqrt{3})+\varphi(r'+s'\sqrt{3}). \end{aligned}$$

Moreover,

$$\begin{aligned} \varphi((r+s\sqrt{3})\cdot(r'+s'\sqrt{3})) &= \varphi((rr'+3ss')+(rs'+r's)\sqrt{3}) \\ &= [(rr'+3ss')+(rs'+r's')x] \\ &= [r+sx]\cdot[r'+s'x] \\ &= \varphi(r+s\sqrt{3})\cdot\varphi(r'+s'\sqrt{3}). \end{aligned}$$

This shows that $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}[x]/(x^2-3)$ are isomorphic.

9 a. This follows from what we did in problem 1 of Section 5.2. b. I will write the equation as $z^3+z+1=0$. Using the multiplication and addition tables from problem 1 in Section 5.2, we have $z=[x],[x^2],[x^2+x]$ are all roots of z^3+z+1. So there are three roots in this field.

10. We argue by contradiction. If there were such an isomorphism φ, then we note first that since φ is surjective, $\varphi([1])=[1]$ by one of our general properties of ring homomorphisms. Hence by the homomorphism properties. $\varphi([n])=[n]$ for all $n\in\mathbb{Z}$. Now, there would have to be some $[ax+b]\in\mathbb{Q}[x]/(x^2-2)$ that maps to $[x]\in\mathbb{Q}[x]/(x^2-3)$. This implies $\varphi([ax+b]^2)=[x]^2=[3]$. But then, $[ax+b][ax+b]=[2abx+b^2+2a^2]=[3]$ in $\mathbb{Q}[x]/(x^2-2)$ also. We claim this cannot happen for the following reason. We must have $2ab=0$ and $b^2+2a^2=3$. These equations have no solutions in the rational numbers: the first says $a=0$ or $b=0$, and then either way there is no solution of the second there are no rational numbers r with $r^2=3$ or $r^2=\frac{3}{2}$.