Mathematics 351 – Abstract Algebra 1
Solutions for Problem Set 6
October 18, 2007

Section 6.1

2. We let

$$I = \{p(x) = a_0 + a_1 x + \cdots \in \mathbb{Z}[x] : a_0 \text{ is even}\}.$$

I is clearly nonempty since $0, 2, 4 + x^2 \in I$ and so forth. Moreover, if $p(x) = a_0 + a_1 x + \cdots$ and $q(x) = b_0 + b_1 x + \cdots$ are in I, then $p(x) - q(x) = a_0 - b_0 + (a_1 - b_1)x + \cdots$. Since a_0, b_0 are divisible by 2, so is $a_0 - b_0$. Hence I is closed under differences. If $r(x) = c_0 + c_1 x + \cdots$ is an arbitrary polynomial in $\mathbb{Z}[x]$, and $p(x)$ as above is in I, then $r(x)p(x) = a_0 c_0 + (a_0 c_1 + a_1 c_0)x + \cdots$. Since a_0 is divisible by 2, so is $a_0 c_0$. Hence I is closed under multiplication by arbitrary $r(x) \in \mathbb{Z}[x]$. This shows I is an ideal by the definition.

6.

a. The set of nonunits in $\mathbb{Z}_8$ is $I = \{0, 2, 4, 6\}$. This (nonempty!) set is closed under differences and products by arbitrary elements in $\mathbb{Z}_8$. This is true because these are the classes of the even numbers mod 8. Since 8 is also even, $a \equiv 2k \bmod 8$ and $b \equiv 2\ell \bmod 8$ implies $a - b \equiv 2(k - \ell) \bmod 8$. If $2(k - \ell) \equiv c \bmod 8$, then $2(k - \ell) - c = 8m$ for some integer m. But then $c = 2(k - \ell) - 8m$ is also even. Similarly if r is an arbitrary class mod 8, and $a \equiv 2k \bmod 8$, then if $2rk \equiv c \bmod 8$, we have $2k - c = 8m$ for some integer m, so c is also divisible by 2.

b. The set of nonunits in $\mathbb{Z}_9$ is $I = \{0, 3, 6\}$. This is an ideal for a similar reason to what happened in part a – this is the set of classes of numbers divisible by 3 in $\mathbb{Z}_9$.

7.

a. In $\mathbb{Z}_5$, $(0) = \{0\}$, and $(1) = (2) = (3) = (4) = \mathbb{Z}_5$.

b. In $\mathbb{Z}_9$, $(0) = \{0\}$, $(1) = (2) = (4) = (5) = (7) = (8) = \mathbb{Z}_9$, and $(3) = (6) = \{0, 3, 6\}$.

c In $\mathbb{Z}_{12}$, $(0) = \{0\}$, $(1) = (5) = (7) = (11) = \mathbb{Z}_{12}$, $(2) = (10) = \{0, 2, 4, 6, 8, 10\}$, $(3) = (9) = \{0, 3, 6, 9\}$, $(4) = (8) = \{0, 4, 8\}$, and $(6) = \{0, 6\}$.

12.

a An example is $(2) = (-2)$. This follows since every even integer $n = 2k$ is also $n = (-2)(-k)$, and vice versa. (This is the *only* way the equality $(c) = (d)$ can happen if $c \neq d$ in $\mathbb{Z}$, since $c \in (d)$ says $c = dm$ for some integer m. Conversely, $d \in (c)$ says $d = cn$ for some integer n. Then substituting, we see $c = c(nm)$, so $nm = 1 \in \mathbb{Z}$. This is only possible if $n = m = 1$ or $n = m = -1$.)

b To show the equality, we show inclusions in both directions. $\subseteq$: Let $n \in (4,6)$. Then $n = 4a + 6b$ for some integers a, b. But then $n = 2(2a + 3b)$, and $2a + 3b \in \mathbb{Z}$, so $n \in (2)$. $\supseteq$: Note that $2 = 4(-1) + 6(1) \in (4,6)$. Then for all $n \in \mathbb{Z}$, $2n = 4(-n) + 6(n) \in (4,6)$. Hence $(2) \subseteq (4,6)$.

c Similar to part b. First we show $\subseteq$: Let $n \in (6,9,15)$. Then $n = 6a+9b+12c = 3(2a+3b+4c)$ for some $a, b, c \in \mathbb{Z}$. This shows $(6,9,15) \subseteq (3)$. On the other hand, to show $\supseteq$: since $3 = 6(-1) + 9(1)$, we have $3n = 6(-n) + 9(n) + 12(0) \in (6,9,15)$. *Comment:* Note that this argument actually shows somewhat more than the problem asked. In fact $(6,9) = (3)$, and the third generator is unnecessary.

13.

a. If $1_R \in I$ and I is an ideal, then for all $r \in R$, $r \cdot 1_R = r \in I$. Hence $R \subseteq I$. Since $I \subseteq R$ by definition, this shows $I = R$.

b. If $u \in I$ and u is a unit, then say $a \in R$ satisfies $au = 1_R$. By definition, since I is an ideal, $au \in I$, so $1_R \in I$, and $I = R$ by part a.

14. Let I be an ideal in a field F, and let $I \neq (0_F) = \{0_F\}$. Then there is some $a \neq 0_F$ in I. But then since F is a field, a is a unit in F, and then $I = F$ by problem 13.

21.

a. $I = \{0,3\}$ is clearly nonempty, and closed under differences and products by arbitrary elements in $\mathbb{Z}_6$. (A formal proof would proceed as in 6 a above.) The distinct cosets are $0 + I = I = 3 + I$, $1 + I = \{1,4\} = 4 + I$, and $2 + I = \{2,5\} = 5 + I$.

b. $I = \{0,3,6,9,12\}$ is clearly nonempty, and closed under differences and products by arbitrary elements in $\mathbb{Z}_{15}$ (since this subset consists of the classes of multiples of 3 mod 15). (A formal proof would proceed as in 6 a above.) The distinct cosets are $0+I = I$, $1+I = \{1,4,7,10,13\}$, and $2 + I = \{2,5,8,11,14\}$.

23. $I \neq \emptyset$ since $r = 0_R$ satisfies $0_R t = 0_R$ for all $t \in J$. Hence $0_R \in I$. Next, let $a, b \in I$. Then $at = 0_R$ and $bt = 0_R$ for all $t \in J$. But then for all $t \in J$, $(a-b)t = at - bt = 0_R - 0_R = 0_R$. This shows that $a - b \in I$. Finally let $a \in I$ and $r \in R$. By associativity, we have $(sa)t = s(at) = s \cdot 0_R = 0_R$ for all $t \in J$. Hence $sa \in I$. Similarly for all $t \in J$, $(as)t = a(st)$. Now J is an ideal in R and $s \in R$ so $st \in J$. Hence $a(st) = 0_R$. This shows $as \in I$ also. By definition, I is an ideal in R.

24. $K \neq \emptyset$ since $a = 0_R$ satisfies $r0_R = 0_R$ for all $r \in R$. J is an ideal so $0_R \in J$, and hence $r0_R \in J$ for all $r \in R$. Hence $0_R \in K$. Next, let $a, b \in K$. Then $ra \in J$ and $rb \in J$ for all $r \in R$. But then for all $r \in R$, $r(a-b) = ra - rb \in J$, since J is closed under differences. This shows that $a - b \in K$. Finally let $a \in K$ and $s \in R$. By associativity, we have $r(sa) = (rs)a \in J$ since $rs \in R$. Hence

$sa \in K$. Similarly for all $r \in R$, $r(as) = (ra)s$. Now $ra \in J$, and J is an ideal in R so $(ra)s \in J$. Hence $as \in K$. By the definition, K is an ideal in R.

38. If $I = \{0\}$, then $I = (0)$ is principal. Hence we may assume now that $I \neq \{0\}$. We claim that I always contains positive elements in this case. This is true since I must contain some $n \neq 0$. If $n > 0$, then we are done. If $n < 0$, then $(-1)(n) = -n > 0$ and $-n \in I$ as well. Now, by the Well-Ordering Principle, there is a smallest strictly positive element in I, call it c. We will show that $I = (c)$, so I is principal. The $\supseteq$ inclusion is automatic since $c \in I$ implies $ck \in I$ for all $k \in \mathbb{Z}$. For the other ($\subseteq$) inclusion, let $n \in I$, and divide c into n by integer division: $n = qc + r$, where $0 \leq r < c$. However this equation shows $r = n - qc$. Since $n, c \in I$, this implies $r \in I$ as well. However, c was the smallest strictly positive element in I, so the possibility is $r = 0$. This shows $n = qc \in (c)$ so $I \subseteq (c)$. Therefore $I = (c)$ is a principal ideal.

39.

a. S is nonempty since $0 = \frac{0}{1} \in S$. If $\frac{a}{b}, \frac{c}{d} \in S$, then the difference $\frac{a}{b} - \frac{c}{d} = \frac{da-bc}{bd}$. To put this in lowest terms, we would compute the gcd of the top and bottom, say $n = (da - bc, bd)$. Then we have $\frac{da-bc}{bd} = \frac{nA}{nB} = \frac{A}{B}$ where $(A, B) = 1$. Note that since $B|(bd)$ and b, d are odd, then B must also be odd. Hence $\frac{a}{b} - \frac{c}{d} \in S$. Similarly, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. To put this in lowest terms, we would compute the gcd of the top and bottom, say $n = (ac, bd)$. Then we have $\frac{ac}{bd} = \frac{nA}{nB} = \frac{A}{B}$ where $(A, B) = 1$. Note that $B|(bd)$ must be odd since b, d are odd. Hence $\frac{a}{b} \cdot \frac{c}{d} \in S$.

b. Let I be the set of elements of S with even numerators. I is nonempty since $0 = \frac{0}{1} \in I$. I is closed under differences, since if $\frac{2k}{b}, \frac{2\ell}{d} \in I$, then $\frac{2k}{b} - \frac{2\ell}{d} = \frac{2(dk-b\ell)}{bd}$. If this is not already in lowest terms, then we might have to cancel some common factors. However note that bd is odd so $2 \not| (bd)$. Hence, because of unique factorization in $\mathbb{Z}$, the factor of 2 on the top will remain after any common factors are cancelled. This shows that I is closed under differences. Similarly, if $\frac{2k}{b} \in I$, and $\frac{c}{d} \in S$, then $\frac{2k}{b} \cdot \frac{c}{d} = \frac{2kc}{bd}$. If this is not already in lowest terms, then we might have to cancel some common factors. However note that bd is odd so $2 \not| (bd)$. Hence the factor of 2 on the top will remain after any common factors are cancelled. Thus I is an ideal in S.

c. We claim that $1 + I$ is the only coset of I different from I itself, and we will show that by showing that $1 + I$ coincides with the set of all elements of S where the numerator is *odd*. (Since every element of S either has an even numerator or an odd numerator, there cannot be any additional cosets.) Note first that $1 + \frac{2k}{b} = \frac{b+2k}{b}$ has an odd numerator so $1 + I$ is contained in the set of elements in S with odd numerators. Conversely, if $\frac{2k+1}{b}$ has an odd numerator, then we can rewrite this as $\frac{2k+1}{b} = 1 + \frac{2k+1-b}{b}$ Since b is odd, $2k + 1 - b$ is even so $\frac{2k+1-b}{b}$ is in I. Hence $\frac{2k+1}{b} \in 1 + I$.

40. Notice that 39 is the special case of 40 where $p = 2$. The proofs of the more general statements here are similar. To prepare, note that the fact used in the proof of 39 that b, d odd implies bd odd carries over to this setting because of the contrapositive form of Euclid's Lemma in $\mathbb{Z}$: If p is prime and $p \not| b$ and $p \not| d$, then $p \not| (bd)$.

a. T is nonempty since $0 = \frac{0}{1} \in S$. If $\frac{a}{b}, \frac{c}{d} \in T$, then the difference $\frac{a}{b} - \frac{c}{d} = \frac{da-bc}{bd}$. To put this in lowest terms, we would compute the gcd of the top and bottom, say $n = (da - bc, bd)$. Then we have $\frac{da-bc}{bd} = \frac{nA}{nB} = \frac{A}{B}$ where $(A, B) = 1$. Note that since $B|(bd)$ and b and d are not divisible by p, then bd and hence B must also be not divisible by p. Hence $\frac{a}{b} - \frac{c}{d} \in T$. Similarly, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. To put this in lowest terms, we would compute the gcd of the top and bottom, say $n = (ac, bd)$. Then we have $\frac{ac}{bd} = \frac{nA}{nB} = \frac{A}{B}$ where $(A, B) = 1$. Note that $B|(bd)$ must be not divisible by p since b, d are not divisible by p. Hence $\frac{a}{b} \cdot \frac{c}{d} \in T$.

b. Let I be the set of elements of T with numerators divisible by p. I is nonempty since $0 = \frac{0}{1} \in I$. I is closed under differences, since if $\frac{pk}{b}, \frac{p\ell}{d} \in I$, then $\frac{pk}{b} - \frac{p\ell}{d} = \frac{p(dk-b\ell)}{bd}$. If this is not already in lowest terms, then we might have to cancel some common factors. However note that b and d are not divisible by p, so $p \not| (bd)$. Hence, because of unique factorization in $\mathbb{Z}$, the factor of p on the top will remain after any common factors are cancelled. This shows that I is closed under differences. Similarly, if $\frac{pk}{b} \in I$, and $\frac{c}{d} \in T$, then $\frac{pk}{b} \cdot \frac{c}{d} = \frac{pkc}{bd}$. If this is not already in lowest terms, then we might have to cancel some common factors. However note that bd is divisible by p so $p \not| (bd)$. Hence the factor of p on the top will remain after any common factors are cancelled. Thus I is an ideal in T.

c. We claim that $0 + I, 1 + I, 2 + I, \ldots, (p-1) + I$ are the only cosets of I. We will show that by showing that every element of T belongs to one of these cosets. This is significantly trickier than the corresponding statement in 39, though(!) To see it, we need to recall from Algebraic Structures that an integer b has a multiplicative inverse mod p exactly when $(b, p) = 1$ or $p \not| b$. So let $\frac{a}{b} \in T$. We claim that this element belongs to the coset $s + I$ where $s \in \{0, 1, \ldots, p-1\} \equiv ua \bmod p$, where u is the multiplicative inverse of b mod p: $ub \equiv 1 \bmod p$. To see this, write $a = qp + i$ with $i \in \{0, 1, \ldots, p-1\}$, and $ub = 1 + kp$. Then

$$\frac{a}{b} = \frac{i + qp}{b} = \frac{i(ub - kp) + qp}{b} = ui + \frac{p(q - ki)}{b} \in ui + I.$$

But now $ui \equiv ua \equiv s \mod p$, so $ui = s + \ell p$ for some $\ell \in \mathbb{Z}$ and hence

$$\frac{a}{b} = s + \left(\frac{p\ell}{1} + \frac{p(q - ki)}{b}\right) \in s + I.$$

This establishes our claim.

Section 6.2

2. By the First Isomorphism Theorem, if $\varphi : F \to S$ is any ring homomorphism, then $\mathrm{im}(\varphi) \simeq F/\ker(\varphi)$. Moreover $\ker(\varphi)$ is an ideal in F. By 6.1/14, this says $\ker(\varphi) = (0_F)$ or $\ker(\varphi) = F$. In the first case $\mathrm{im}(\varphi) \simeq F/(0_F) \simeq F$ (each element of F defines a distinct coset). In the second case, $\mathrm{im}(\varphi) \simeq F/F = \{0\}$, the zero ring (all elements of F belong to the same coset).

3. Continuing the reasoning from 2, if $f : F \to R$ is a surjective homomorphism and R is not the zero ring, there must be at least two elements in R (0_R and something else). Hence we cannot be

in the second case above since f surjective says $\mathrm{im}(f) = R$. It follows that $\mathrm{im}(f) \simeq F/(0_F) \simeq F$. Since $\ker(f) = (0_F)$, f is injective as well as surjective, hence is an isomorphism.

6.

a. See Section 6.1/7c above. This is the same question(!)

b. We will show the case of $I = (6) = \{0, 6\}$. The others are similar, and simpler, since there are fewer distinct cosets. Here the distinct cosets are $0 + I$, $1 + I$, $2 + I$, $3 + I$, $4 + I$, $5 + I$. The tables for $\mathbb{Z}_{12}/I$ are as follows (writing i for $i + I$ in all cases to save typing!)

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

and

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

For instance, $(2+I)+(5+I) = 7+I = 1+I$ and $(2+I)(5+I) = 10+I = 4+I$. By inspection, we see that this quotient ring is isomorphic to $\mathbb{Z}_6$. Similarly, $\mathbb{Z}_{12}/(0) \simeq \mathbb{Z}_{12}$, $\mathbb{Z}_{12}/(1) \simeq \{0\}$ (the zero ring), $\mathbb{Z}_{12}/(2) \simeq \mathbb{Z}_2$, $\mathbb{Z}_{12}/(3) \simeq \mathbb{Z}_3$, $\mathbb{Z}_{12}/(4) \simeq \mathbb{Z}_4$.

c. This follows from the First Isomorphism Theorem. Every ring homomorphism $\varphi : \mathbb{Z}_{12} \to S$ has $\mathrm{im}(\varphi) \simeq \mathbb{Z}_{12}/I$ for $I = \ker(\varphi)$. Every ideal I in $\mathbb{Z}_{12}$ is one of the six principal ideals found in 6.1/7c. Hence by part b, every homomorphic image of $\mathbb{Z}_{12}$ is isomorphic to one of the rings listed.

8. These can be done by the same method illustrated in the solution for 6b above. To see a less computational method for part a, notice first that I is an ideal by Section 6.1/21a. We have $\mathbb{Z}_6/([3]) = \{[0] + I, [1] + I, [2] + I\}$. Then we define a mapping $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_3$ by $\varphi([i]_6) = [i]_3$ (the added subscripts indicate which ring the congruence class lives in, for clarity). This is well-defined since if $[i]_6 = [j]_6$, then $6|(i - j)$ which implies $3|(i - j)$, so $[i]_3 = [j]_3$. We have that φ is a ring homomorphism since

$$\varphi([i]_6 + [j]_6) = \varphi([i + j]_6) = [i + j]_3 = [i]_3 + [j]_3 = \varphi([i]_6) + \varphi([j]_6),$$

and

$$\varphi([i]_6 \cdot [j]_6) = \varphi([ij]_6) = [ij]_3 = [i]_3 \cdot [j]_3 = \varphi([i]_6) \cdot \varphi([j]_6).$$

We see that φ is surjective since every element in $\mathbb{Z}_3$ is in the image. Finally, $\ker(\varphi) = \{[0]_6, [3]_6\}$. Hence by the First Isomorphism Theorem,

$$\mathbb{Z}_3 = \operatorname{im}(\varphi) \simeq \mathbb{Z}_6/\ker(\varphi) = \mathbb{Z}_6/([3]_6).$$

The proof of part b is exactly analogous and will be omitted.

28. Define $\varphi : S \to \mathbb{Z}_2$ by $\varphi\left(\frac{a}{b}\right) = [a] \in \mathbb{Z}_2$. Since the denominator b is odd, we have $[b] = [1]$ in $\mathbb{Z}_2$. Hence

$$\varphi\left(\frac{a}{b} + \frac{c}{d}\right) = \varphi\left(\frac{ad+bc}{bd}\right) = [ad+bc] = [a][d] + [b][c] = [a] + [c] \in \mathbb{Z}_2.$$

Since this equals $\varphi\left(\frac{a}{b}\right) + \varphi\left(\frac{c}{d}\right)$, the first homomorphism property holds. Similarly,

$$\varphi\left(\frac{a}{b} \cdot \frac{c}{d}\right) = \varphi\left(\frac{ac}{bd}\right) = [ac] = [a] \cdot [c] \in \mathbb{Z}_2.$$

Since this equals $\varphi\left(\frac{a}{b}\right) \cdot \varphi\left(\frac{c}{d}\right)$, the second homomorphism property holds. Now, $\ker(\varphi) = I$ since it is exactly the elements in S with even numerators that map to $[0]$ in $\mathbb{Z}_2$. φ is also surjective since the elements in S with odd numerators map to $[1]$. So by the First Isomorphism Theorem,

$$S/\ker(\varphi) = S/I \simeq \operatorname{im}(\varphi) = \mathbb{Z}_2.$$

29. The idea here is similar to what we did in 28 above. However, as noted in the solution to 6.1/40, this is somewhat trickier. A mapping $\varphi : T \to \mathbb{Z}_p$ that works here is to define $\varphi\left(\frac{a}{b}\right) = [a][b]^{-1} \in \mathbb{Z}_p$. (Recall that $[b]$ has a multiplicative inverse in $\mathbb{Z}_p$ exactly when $(p, b) = 1$ and that is the condition for $\frac{a}{b} \in T$.) This is a ring homomorphism since

$$\begin{aligned}
\varphi\left(\frac{a}{b} + \frac{c}{d}\right) &= \varphi\left(\frac{ad+bc}{bd}\right) \\
&= [ad+bc][bd]^{-1} \\
&= ([a][d] + [b][c])[b]^{-1}[d]^{-1} \\
&= [a][b]^{-1} + [c][d]^{-1} \\
&= \varphi\left(\frac{a}{b}\right) + \varphi\left(\frac{c}{d}\right)
\end{aligned}$$

and

$$\begin{aligned}
\varphi\left(\frac{a}{b} \cdot \frac{c}{d}\right) &= \varphi\left(\frac{ac}{bd}\right) \\
&= [ac][bd]^{-1} \\
&= [a][c][b]^{-1}[d]^{-1} \\
&= ([a][b]^{-1})([c][d]^{-1}) \\
&= \varphi\left(\frac{a}{b}\right) \cdot \varphi\left(\frac{c}{d}\right).
\end{aligned}$$

The kernel of φ is exactly the set of $\frac{a}{b} \in T$ with $[a] = [0] \in \mathbb{Z}_p$, which is I. The image of φ is all of $\mathbb{Z}_p$ since $\varphi\left(\frac{i}{1}\right) = [i]$ for $i = 0, 1, \ldots, p-1$. Hence by the First Isomorphism Theorem, $\mathbb{Z}_p = \operatorname{im}(\varphi) \simeq T/\ker(\varphi) = T/I$.