Mathematics 351 – Abstract Algebra 1
Solutions for Problem Set 2
September 15, 2007

Section 3.3

4. The tables for *addition* mod 10 in S and *addition* mod 5 in $\mathbb{Z}_5$ do correspond under the given mapping $f : \mathbb{Z}_5 \to S$. However, the tables for multiplication mod 10 in S and multiplication in $\mathbb{Z}_5$ do not. In other words for the given mapping $f : \mathbb{Z}_5 \to S$ it is not the case that $f(a \cdot_5 b) = f(a) \cdot_{10} f(b)$ for all $a, b \in \mathbb{Z}_5$. The tables are:

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

and

$\cdot_{10}$	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	2
6	0	2	4	6	8
8	0	6	2	8	4

For example, using Hungerford's notation, note that $f(\overline{2} \cdot_5 \overline{3}) = f(\overline{1}) = 2$, but $f(\overline{2}) = 4$, and $f(\overline{3}) = 6$, so $f(\overline{2}) \cdot_{10} f(\overline{3}) = 4$.

5. The mapping f is injective since $f(a) = f(a')$ implies $(a, 0_S) = (a', 0_S)$, so $a = a'$. It is also surjective since every $(a, 0_S)$ in $\overline{R}$ is $f(a)$ for the $a \in R$ appearing in the first component. Then

$$f(a + b) = (a + b, 0_S) = (a, 0_S) + (b, 0_S) = f(a) + f(b)$$

and

$$f(a \cdot b) = (a \cdot b, 0_S) = (a, 0_S) \cdot (b, 0_S) = f(a) \cdot f(b)$$

by the definition of the operations in $R \times S$. Therefore f is an isomorphism.

10.

a) This is not an homomorphism because $f(a \cdot b) = -(a \cdot b) \neq (-a) \cdot (-b) = f(a) \cdot f(b)$.

b) This is an isomorphism, hence a homomorphism. The reason is that in fact $-x = x$ for all $x \in \mathbb{Z}_2$. This is the same as the identity mapping which is clearly an isomorphism.

c) This is not a homomorphism since, for instance $g(0) = 1 \neq 0$ in $\mathbb{Q}$ shows that the property of Theorem 3.12, part (1) fails for this f.

d) This is not a homomorphism since

$$h(ab) = \begin{pmatrix} -(ab) & 0 \\ ab & 0 \end{pmatrix} \neq \begin{pmatrix} -a & 0 \\ a & 0 \end{pmatrix} \begin{pmatrix} -b & 0 \\ b & 0 \end{pmatrix} = h(a)h(b).$$

e) This is a homomorphism since by the definitions of the ring operations in $\mathbb{Z}_{12}$ and $\mathbb{Z}_4$,

$$f([x]_{12} + [y]_{12}) = f([x+y]_{12}) = [x+y]_4 = [x]_4 + [y]_4 = f([x]_{12}) + f([y]_{12}),$$

and

$$f([x]_{12} \cdot [y]_{12}) = f([x \cdot y]_{12}) = [x \cdot y]_4 = [x]_4 \cdot [y]_4 = f([x]_{12}) \cdot f([y]_{12}).$$

17. Note that S consists of the classes $[x] \in \mathbb{Z}_{28}$ for x divisible by 4. This set is closed under differences and multiplication in $\mathbb{Z}_{28}$, so by the criterion of Theorem 3.6, it is a subring. The mapping $f([x]_7) = [8x]_{28}$ is seen to be injective and surjective by computing the values: $f([0]_7) = [0]_{28}$, and

$$f([1]_7) = [8]_{28}, f([2]_7) = [16]_{28}, f([3]_7) = [24]_{28}, f([4]_7) = [4]_{28}, f([5]_7) = [12]_{28}, f([6]_7) = [20]_{28}.$$

The mapping f is a homomorphism since by the definitions of the ring operations in $\mathbb{Z}_7$ and $\mathbb{Z}_{28}$,

$$f([x]_7 + [y]_7) = f([x+y]_7) = [8(x+y)]_{28} = [8x]_{28} + [8y]_{28} = f([x]_7) + f([y]_7),$$

and since $[8 \cdot 8]_{28} = [64]_{28} = [8]_{28}$:

$$f([x]_7 \cdot [y]_7) = f([x \cdot y]_7) = [8(x \cdot y)]_{28} = [8x]_{28} \cdot [8y]_{28} = f([x]_7) \cdot f([y]_7).$$

19 and 3.1/18. First we show that $\mathbb{Z}^*$ is a ring under the $\oplus, \odot$ operations. (part of 3.1/18). Closure under $\oplus$, and $\odot$ is clear since the elements of $\mathbb{Z}^*$ are just the ordinary integers and $a \oplus b = a+b-1$, $a \odot b = a+b-ab$. $\oplus$ is commutative since $a \oplus b = a+b-1 = b+a-1 = b \oplus a$. $\oplus$ is associative since $(a \oplus b) \oplus c = (a+b-1)+c-1 = a+b+c-2$, while $a \oplus (b \oplus c) = a+(b+c-1)-1 = a+b+c-2$ also. The integer $0_{\mathbb{Z}^*} = 1$ is an identity element for the $\oplus$ operation since $a \oplus 1 = a+1-1 = a$ for all a. Each integer a has an inverse $-(a) = -a+2$ under the $\oplus$ operation since $a \oplus (-a+2) = a-a+2-1 = 1 = 0_{\mathbb{Z}^*}$. $\odot$ is associative since $(a \odot b) \odot c = (a+b-ab)+c-(a+b-ab)c = a+b+c-ab-ac-bc+abc$, while $a \odot (b \odot c) = a+(b+c-bc)-a(b+c-bc) = a+b+c-ab-ac-bc+abc$ also. Finally, we have a distributive law since $a \odot (b \oplus c) = a+(b+c-1)-a(b+c-1) = (a+b-ab)+(a+c-ac)-1 = (a \odot b) \oplus (a \odot c)$. It is not necessary to prove the other distributive property because it easy to see that $\odot$ is commutative as well: $a \odot b = a+b-ab = b+a-ba = b \odot a$ for all a, b.

The ring $\mathbb{Z}^*$ is an integral domain because it is a commutative ring by the previous paragraph, it has a multiplicative identity $1_{\mathbb{Z}^*} = 0$ (because $a \odot 0 = a+0-a \cdot 0 = a$ for all $a \in \mathbb{Z}$), and if $a \odot b = 0^*_{\mathbb{Z}}$, then $a+b-ab = 1$, so $(a-1)(b-1) = 0$, and hence by properties of the usual multiplication in $\mathbb{Z}$, $a = 1 = 0_{\mathbb{Z}^*}$, or $b = 1 = 0_{\mathbb{Z}^*}$. This completes 3.1/18.

Now, consider the mapping $f : \mathbb{Z} \to \mathbb{Z}^*$ defined by $f(x) = 1-x$. f is an injective and surjective mapping because if $y \in \mathbb{Z}^*$ (also an ordinary integer, then there exists exactly one $x \in \mathbb{Z}$ with $f(x) = 1-x = y$, namely $x = 1-y$. Next, we have

$$f(a+b) = 1-(a+b) = (1-a)+(1-b)-1 = f(a) \oplus f(b).$$

Finally,

$$f(a \cdot b) = 1 - ab = (1 - a) + (1 - b) - (1 - a)(1 - b) = f(a) \otimes f(b).$$

Therefore the mapping f is a ring homomorphism, and $\mathbb{Z}$ and $\mathbb{Z}^*$ are isomorphic as rings.

24. The mapping is $g : \mathbb{R} \to M_{2\times 2}(\mathbb{R})$ with

$$g(r) = \begin{pmatrix} 0 & 0 \\ -r & r \end{pmatrix}.$$

This is injective because if $g(r) = g(s)$ for $r, s \in \mathbb{R}$, then

$$\begin{pmatrix} 0 & 0 \\ -r & r \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -s & s \end{pmatrix},$$

which implies $r = s$ (look at the lower right entries). However g is not surjective since not every 2×2 matrix is $g(r)$ for some r (take any matrix A with nonzero entries in the first row, for instance).

27. Let $f : R \to S$ be an isomorphism. Then f is injective and surjective, so it has an inverse function $g : S \to R$. The inverse function of an injective and surjective mapping is itself injective and surjective by "general nonsense" (i.e. this is a direct consequence of the definitions – f is an inverse function for g, so g must also be injective and surjective.) To show that g satisfies the other properties of an isomorphism of rings, let $x, y \in S$. Since f is surjective, there are $a, b \in R$ with $x = f(a)$ and $y = f(b)$, so $g(a) = x$ and $g(b) = y$. Then using the homomorphism properties for f:

$$g(a + b) = g(f(x) + f(y)) = g(f(x + y)) = x + y = g(a) + g(b),$$

and

$$g(a \cdot b) = g(f(x) \cdot f(y)) = g(f(x \cdot y)) = x \cdot y = g(a) \cdot g(b).$$

Hence g is also an isomorphism of rings.

28. We will use the subring criterion of Theorem 3.6. First note that K is always nonempty by part 1 of Theorem 3.12: $f(0_R) = 0_S$, so $O_R \in K$. Next, let $a, b \in K$. Then since f is a homomorphism,

$$f(a - b) = f(a) - f(b) = 0_S - 0_S = 0_S.$$

This shows $a - b \in K$, so K is closed under differences. Similarly,

$$f(a \cdot b) = f(a) \cdot f(b) = 0_S \cdot 0_S = 0_S.$$

This shows $a \cdot b \in K$ so K is closed under products. Therefore K is a subring of R.

29. This very similar to 28. We again use the subring criterion of Theorem 3.6. First note that P is always nonempty by part 1 of Theorem 3.12: $f(0_R) = 0_S \in T$, so $O_R \in P$. Next, let $a, b \in P$, so $f(a), f(b) \in T$. Then since f is a homomorphism,

$$f(a - b) = f(a) - f(b) \in T,$$

since $f(a), f(b) \in T$ and T is a subring of S. This shows $a - b \in P$, so P is closed under differences. Similarly,

$$f(a \cdot b) = f(a) \cdot f(b) \in T,$$

since T is a subring of S. This shows $a \cdot b \in P$ so P is closed under products. Therefore P is a subring of R.

Section 4.1

5.

a) $q(x) = 3x^2 - 5x + 8$, and $r(x) = -4x - 6$.

c) $q(x) = x^3 + 3x^2 + 2x + 3$ and $r(x) = 4$.

14.

a) Consider what happens at each step of the division process. If the leading term of the intermediate dividend polynomial is ax^s and the leading term of g is ux^r, where u is a unit in R, then the term that goes into the quotient is $u^{-1}ax^{s-r}$, and the process proceeds exactly as in the case of polynomials with coefficients in a field F.

b) Consider $f = x + 1$ and $g = 2x + 1$. There are no integer polynomials q, r as in the statement of the division algorithm because if q is any nonzero polynomial with integer coefficients, the leading term of qg will have a coefficient that is divisible by 2. Hence f cannot be written as $f = qg + r$ with $\deg(r) < \deg(g)$ or $r = 0$. *Comment:* When $q \neq 0$, the leading term in $qg + r$ will come from qg in the situation of the division algorithm because of the condition $\deg(r) < \deg(g)$, or $r = 0$. This follows because $\deg(qg) \geq \deg(g)$.

17. φ is surjective because every $[a_m]x^m + \cdots + [a_0] \in \mathbb{Z}_n[x]$ is $\varphi(a_m x^m + \cdots + a_0)$, for the polynomial $a_m x^m + \cdots + a_0 \in \mathbb{Z}[x]$. We next show φ is a homomorphism. First, if $f = a_m x^m + \cdots + a_0$ and $g = b_k x^k + \cdots + b_0$, then $f + g$ is the polynomial where for each $\ell \geq 0$, the coefficient of x^ℓ is $a_\ell + b_\ell$. Hence the coefficient of x^ℓ in $\varphi(f+g)$ is $[a_\ell + b_\ell] = [a_\ell] + [b_\ell] \in \mathbb{Z}_n$. This shows $\varphi(f+g) = \varphi(f) + \varphi(g)$. Similarly, in the polynomial $f \cdot g$, for each $\ell \geq 0$, the coefficient of x^ℓ is $\sum_{i=0}^{\ell} a_i b_{\ell - i}$. Hence using the definition of the sum and product in $\mathbb{Z}_n$, the coefficient of x^ℓ in $\varphi(f \cdot g)$ is

$$\left[\sum_{i=0}^{\ell} a_i b_{\ell-i}\right] = \sum_{i=0}^{\ell} [a_i][b_{\ell-i}],$$

which is the coefficient of x^ℓ in $\varphi(f) \cdot \varphi(g)$. This shows $\varphi(f \cdot g) = \varphi(f) \cdot \varphi(g)$.

18. D is neither a homomorphism of rings, nor an isomorphism. This can be seen because D does not satisfy the multiplicative property of homomorphisms. For example $D(x \cdot x) = D(x^2) = 2x \neq D(x) \cdot D(x) = 1$. *Comment:* Of course, D also fails to be injective, since $D(1) = 0 = D(0)$, but $1 \neq 0$.

Section 4.2

5 b) Here is a Maple session carrying out the computations of the remainders in the Euclidean Algorithm:

```
> f := x^5+x^4+2*x^3-x^2-x-2;
                    5    4      3    2
                   x  + x  + 2 x  - x  - x - 2
> g := x^4+2*x^3+5*x^2+4*x+4;
                     4      3      2
                    x  + 2 x  + 5 x  + 4 x + 4
> r1 := rem(f, g, x);
                                3
                             2 - x  - x
> r2 := rem(g, r1, x);
                                 2
                           8 + 4 x  + 4 x
> r3 := rem(r1, r2, x);
                                0
```

The last nonzero remainder, made monic, is the gcd, so

$$\gcd(f, g) = x^2 + x + 2.$$

14. Since f, g are relatively prime, $\gcd(f, g) = 1$. Hence there are polynomials $u, v \in F[x]$ such that $1 = uf + vg$. Multiplying by h on both sides, we get

$$h = ufh + vgh. \tag{1}$$

Now if $f|h$, then $h = kf$ for some polynomial $k \in F[x]$. Similarly, if $g|h$ then $h = \ell g$ for some polynomial $\ell \in F[x]$. Substitute $h = \ell g$ for the h in the first h in (1) and $h = kf$ for the second. We get $h = uf\ell g + vgkf = h$. Hence $h = (u\ell + vk)(fg)$. Since $u\ell + vk \in F[x]$, this shows $(fg)|h$.

15. We assume $\gcd(f, g) = 1$. Hence there are $u, v \in F[x]$ with $uf + vg = 1$. Now if $h|f$, then $f = hk$ for some $k \in F[x]$. But then $(uk)h + vg = 1$. This shows that $1 \in S = \{Uh + Vg : U, V \in F[x]\}$. By the proof of Theorem 4.5, it follows that $1 = \gcd(h, g)$, so h and g are relatively prime.