Mathematics 351 – Abstract Algebra I
Solutions for Problem Set 1
September 8, 2007

Section 3.1

8. a) $\overline{R} = \{(0,0),(1,0),(2,0)\}$ and $\overline{S} = \{(0,0),(0,1),(0,2),(0,3),(0,4)\}$.

b) (Note that the question says "for all rings R, S"). To save some writing, we will use the subring criterion from Theorem 3.6 in the next section. $\overline{R}$ is nonempty since R is. Let $(a,0_S),(b,0_S) \in \overline{R}$. Then $(a,0_S)-(b,0_S) = (a-b, 0_S-0_S) = (a-b,0_S)$. Since R is a ring, $a-b \in R$. Hence $\overline{R}$ is closed under differences. Similarly, $(a,0_S)\cdot(b,0_S) = (a\cdot b, 0_S\cdot 0_S) = (a\cdot b, 0_S)$. Since R is a ring $a\cdot b \in R$. Hence $\overline{R}$ is closed under products. It follows that $\overline{R}$ is a subring of $R \times S$.

c. The proof is similar to the proof of b.

9. Again we will use the criterion from Theorem 3.6. Let $a+b\sqrt{2}, c+d\sqrt{2}$ be in $\mathbf{Z}[\sqrt{2}]$, which is clearly nonempty. Then

$$(a+b\sqrt{2}) - (c+d\sqrt{2}) = (a-c) + (b-d)\sqrt{2}$$

Since a,c,b,d are integers, so are $a-c$ and $b-d$. Thus $\mathbf{Z}[\sqrt{2}]$ is closed under differences. Similarly,

$$(a+b\sqrt{2})\cdot(c+d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = (ac+2bd) + (ad+bc)\sqrt{2}$$

Since a,c,b,d are integers, so are $ac+2bd$ and $ad+bc$. Thus $\mathbf{Z}[\sqrt{2}]$ is closed under products and a subring of $\mathbf{R}$.

11. See the answer in the text. *Note:* When answers are given like this, they are *only* to help you check your work. To get full credit, you must show more details than given in the textbook. For calculational problems like this, include full details for at least some parts.

16. Closure under sums and products follows by constructing the operation tables, or by noting that the sum and product of integers divisible by 3 is divisible by 3, and the same is true when we take classes mod 18, since 18 is also divisible by 3 (if $3|n$ then $3|r$ where $n = 18q + r$ by division). $0 \in R$ by construction, and each element of R has an additive inverse in R ($-0 = 0$, $-3 = 15$, $-6 = 12$, $-9 = 9$, $-12 = 6$, and $-15 = 3$). Thus R is a subring of $\mathbf{Z}_{18}$ by the criterion from Theorem 3.2 in the text.

Section 3.2

1 a) In a general ring R, we have distributive laws, but we do not assume R is commutative, so

$$(a+b)(a-b) = a^2 + ba - ab - b^2$$

b) Similarly,

$$(a+b)^3 = (a+b)(a^2+ab+ba+b^2) = a^3+a^2b+aba+ab^2+ba^2+bab+b^2a+b^3.$$

c) If R is commutative, then we simplify to the usual forms $(a+b)(a-b) = a^2-b^2$ and $(a+b)^3 = a^3+3a^2b+3ab^2+b^3$.

2. a) There are infinitely many different idempotent 2×2 matrices. Four of them are the matrices:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

b) The classes of $0, 1, 4, 9$ are all of the idempotents in $\mathbf{Z}_{12}$. For example,

$$9^2 = 81 \equiv 9 \pmod{12},$$

since $81 - 9 = 72 = 6 \cdot 12$, which shows that the class of 9 is an idempotent mod 12.

c) Let e be an idempotent in an integral domain R. Then $e^2 = e$, which implies $e^2 - e = 0_R$. Factoring on the left, this shows $e(e-1_R) = 0_R$. Since we assume R is an integral domain, this shows either $e = 0_R$, or $e - 1_R = 0_R$. The second case is equivalent to $e = 1_R$.

8. a) Almost any randomly chosen matrix will fail to commute with some matrix. Matrices that do commute with every matrix are any matrix of the form $\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$ for $r \in \mathbf{R}$.

b) We must show that the given C is a subring of R. We will use the criterion of Theorem 3.6. First note that C is always nonempty since it contains at least 0_R (part 1 of Theorem 3.5 in the text). Let $a, b \in C$. Then $ar = ra$ and $br = rb$ for all $r \in R$. Then using other parts of Theorem 3.5 and the above,

$$(a-b)r = ar - br = ra - rb = r(a-b)$$

for all $r \in R$. It follows that $a - b \in C$. Similarly, using associativity and the equations $ar = ra$, $br = rb$,

$$(ab)r = a(br) = a(rb) = (ar)b = (ra)b = r(ab)$$

for all $r \in R$. Hence $ab \in C$, and C is a subring of R.

10. The statement is *false*, which can be seen by considering the counterexample $R = \mathbf{Z}$. The set of units in $\mathbf{Z}$ is easily seen to be $U = \{1, -1\}$ (no other nonzero integer has a multiplicative inverse in $\mathbf{Z}$). U is not closed under sums: $1 + -1 = 0$. Hence U is not a subring of $\mathbf{Z}$.

12. For this problem, we need to recall a number of facts about integers, divisibility, and gcds that were covered in Algebraic Structures (MATH 243), or Chapters 1 and 2 of Hungerford (see Theorem 1.3 on page 9 in particular). First, the notation (a, n) is

shorthand for the *greatest common divisor* of a, n in $\mathbf{Z}$. Second, for all integers a, b not both zero, (a, b) is the smallest positive integer in the set $\{ua + vb | u, v \in \mathbf{Z}\}$. Hence, in particular, the gcd itself can be written in the form $(a, b) = ua + vb$ for some integers u, v. Finally note that each part is an "if and only if" statement, so we must prove both implications.

a) $\Rightarrow$: Let $[a]$ be a unit in $\mathbf{Z}_n$. This means that there is some $[u]$ in $\mathbf{Z}_n$ such that $[u][a] = [1]$ in $\mathbf{Z}_n$ (since $[1]$ is the multiplicative identity in this ring). But this says $ua \equiv 1 \pmod{n}$, so as an equation in $\mathbf{Z}$, $au - 1 = (-v)n$ for some integer v. This last equation shows $ua + vn = 1$. By the fact about the gcd mentioned above, this implies that $(a, n) = 1$.

$\Leftarrow$: Assume that $(a, n) = 1$. Then there are integers u, v such that $ua + vn = 1$. This can be rearranged to say $ua \equiv 1 \pmod{n}$, so $[u][a] = [1]$ in $\mathbf{Z}_n$. It follows that $[a]$ is a unit in $\mathbf{Z}_n$.

b) $\Rightarrow$: Assume that $[a]$ is a nonunit in $\mathbf{Z}_n$. By part a, this means that $(a, n) = d > 1$ in $\mathbf{Z}$. By the definition of the gcd, we have $a = dp$ and $n = dq$ for some integers p, q. We may assume $0 < a < n - 1$ if we like. From $n = dq$, since $d > 1$, it follows that $[q] \neq [0]$ in $\mathbf{Z}_n$. Multiplying by q on both sides of the equation $a = dp$, we get:

$$qa = q(dp) = (dq)p = np.$$

Hence $[q][a] = [0]$ in $\mathbf{Z}_n$. This implies $[a]$ is a zero divisor in $\mathbf{Z}_n$ (if $[a] \neq [0]$).

$\Leftarrow$: If $[a] \neq [0]$ is a zero divisor in $\mathbf{Z}_n$, there is some $[b] \neq [0]$ such that $[a][b] = [0]$ in $\mathbf{Z}_n$. If $[a]$ was a unit, then we could multiply both sides of this equation by $[u] = [a]^{-1}$ and we would obtain the contradiction $[b] = [0]$. Hence $[a]$ cannot be a unit. (*Comment:* This last reasoning also shows that in any ring a zero divisor cannot also be a unit.)

18. (A different method from the hint.) $0_R \in S$ because S is a subring and is closed under differences. The element 0_R satisfies $0_R + a = a$ for all $a \in S$, so it is an additive identity for S. Then $0_R = 0_S$ by the uniqueness of the additive identity in a ring (see Theorem we proved in class on Wednesday, September 5).

19. a) Consider $R = \mathbf{Z}_6$ and $S = \{0, 2, 4\}$. Then it is easy to see S is a subring of R. Since $0 \cdot 4 = 0$, $2 \cdot 4 = 2$, and $4 \cdot 4 = 4$ in $\mathbf{Z}_6$, 4 is a multiplicative identity for S which is different from the identity $1 \in R$.

b) Let $a \neq 0$ be an element of the subfield S (there must be such an element by the definition of a field). Then we have $a \cdot 1_S = a$ and $a \cdot 1_R = a$, so $a \cdot (1_S - 1_R) = 0_R$. Multiply both sides by the multiplicative inverse a^{-1} from R. We get $1_S - 1_R = 0_R$, so $1_S = 1_R$. (*Comment:* Actually, we only used the hypothesis that R is a field.)

c) Because 1_S is a multiplicative identity for S, we have $1_S \cdot 1_S = 1_S$. Similarly, since 1_R is a multiplicative identity for R and $1_S \in R$, $1_S \cdot 1_R = 1_S$. Subtracting these equations gives $1_S \cdot (1_S - 1_R) = 0_R$. This equation shows that if $1_S \neq 1_R$, then 1_S is a zero-divisor in R. (*Comment:* the statement "if p, then q or r" is logically equivalent to "if p and not q, then r".)

31. *Comment:* For this question and the next one, you need to look at the definition of $n \cdot a$ for $n \in \mathbf{Z}$ and $a \in R$ from page 59 of the text. This is *not* a product using the multiplication in the ring R. It is a shorthand notation the *sum* $a + a + \cdots + a$ (n terms).

a) In $\mathbf{Z}$, we never have $1 + 1 + \cdots + 1 = 0$, if there are $n \geq 1$ terms. Hence $\mathbf{Z}$ has characteristic zero. In $\mathbf{Z}_n$, we have $1 + 1 + \cdots + 1 = 0$ (n 1's), and this is the smallest number of 1's that adds up to 0. Hence the characteristic is n.

b) The additive and multiplicative identities are $(0, 0), (1, 1)$ respectively. Adding n $(1, 1)$'s together will only give $(0, 0)$ in $\mathbf{Z}_4 \times \mathbf{Z}_6$ when n is a multiple of 4 and a multiple of 6 simultaneously. Hence the characteristic of $\mathbf{Z}_4 \times \mathbf{Z}_6$ is $\text{lcm}(4, 6) = 12$.

32. Let R be a finite ring with identity, and consider the elements $n \cdot 1_R$ for all $n \geq 1$. Since there are infinitely many integers n but only finitely many different elements in R, if we compute the $n \cdot 1_R$ for each $n \geq 1$ in turn, at some point, we must obtain a "repeat" of an element previously seen: $m \cdot 1_R = k \cdot 1_R$ for some $1 \leq k < m$. From the definition, we have $(m - k) \cdot 1_R = 0_R$, and $m - k > 0$. Hence

$$S = \{n > 0 \mid n \cdot 1_R = 0_R\}$$

is a nonempty set of natural numbers. By the Well-Ordering Property it has a smallest element, which is the characteristic of R.