

Homework #6 Solutions

Math 312-A

Due Tuesday, March 13, 2007

page 174, #7, 8, 11, 12: Decide whether the indicated operations of addition and multiplication are defined (closed) on the set, and give a ring structure. If a ring is not formed, tell why this is the case. If a ring is formed, state whether the ring is commutative, whether it has unity, and whether it is a field.

page 174, #7: $n\mathbb{Z}$ with the usual addition and multiplication.

$n\mathbb{Z}$ is a ring: $(n\mathbb{Z}, +, 0)$ is an abelian group, multiplication is closed $(nx)(ny) = n(nxy)$ and associative, and the distributive laws hold true for all integers. It is a commutative ring since integer multiplication is commutative. It does not have unity, since there is no nx in it such that $(nx)(ny) = ny$ for all ny in the ring. It is not a field since it lacks unity.

page 174, #8: \mathbb{Z}^+ with the usual addition and multiplication.

The set is not an abelian group with respect to addition, since there are no negative numbers included. Therefore it is not a ring.

page 174, #11: $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ with the usual addition and multiplication.

The set is an abelian group with respect to addition: it is closed, it contains 0, negatives, and is associative and commutative since it is a subset of the real numbers.

It is closed under multiplication: $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$, and the multiplication is associative since it is a subset of the real numbers.

It satisfies the distributive laws since it is a subset of the real numbers.

Therefore the set is a ring.

It is commutative, since multiplication of real numbers is commutative. It has unity: $1 + 0\sqrt{2}$. It is not a field, since $\sqrt{2} = 0 + 1\sqrt{2}$ does not have any inverse:

$$\begin{aligned}\sqrt{2}(a + b\sqrt{2}) &= 2b + a\sqrt{2} \\ &\neq 1 + 0\sqrt{2}\end{aligned}$$

for any integers a and b .

page 174, #12: $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ with the usual addition and multiplication.

As in problem #11, the set is a commutative ring with unity. It is also a field: we can show that every element in it has a multiplicative inverse.

$$\begin{aligned}(a + b\sqrt{2})\left(\frac{a}{a^2 - 2b^2} - \frac{b\sqrt{2}}{a^2 - 2b^2}\right) &= (a + b\sqrt{2})\left(\frac{a - b\sqrt{2}}{a^2 - 2b^2}\right) \\ &= \frac{a^2 - 2b^2}{a^2 - 2b^2} \\ &= 1\end{aligned}$$

where the denominator can not be 0 since if it were, $\sqrt{2} = \pm a/b$ would be a rational number.

page 174, #37: Show that if U is the collection of all units in a ring $\langle R, +, \cdot \rangle$ with unity, then $\langle U, \cdot \rangle$ is a group.
[Warning: Be sure to show that U is closed under multiplication.]

Let $a, b \in U$. Then a^{-1} and b^{-1} exist, and $(ab)^{-1} = b^{-1}a^{-1}$. Therefore ab is also a unit, and U is closed under multiplication.

Multiplication is associative since R is a ring.

There is a multiplicative identity since R is a ring with unity.

a^{-1} is also a unit since its inverse is a .

Therefore U is a group.

page 174, #38: Show that $a^2 - b^2 = (a + b)(a - b)$ for all a and b in a ring R if and only if R is commutative.

We will apply the distributive laws.

$$\begin{aligned}(a + b)(a - b) &= a(a - b) + b(a - b) \\ &= a^2 - ab + ba - b^2\end{aligned}$$

This is equal to $a^2 - b^2$ if and only if $-ab + ba$ is 0, i.e., if $ba = ab$ for all a and b and the ring is commutative.

page 182, #11: Let R be a commutative ring with unity of characteristic 4. Compute and simplify $(a + b)^4$ for $a, b \in R$.

Since R is commutative, we can use the Binomial Theorem.

$$\begin{aligned}(a + b)^4 &= \sum_{k=0}^4 \binom{4}{k} a^{4-k} b^k \\ &= \binom{4}{0} a^4 + \binom{4}{1} a^3 b + \binom{4}{2} a^2 b^2 + \binom{4}{3} a b^3 + \binom{4}{4} b^4 \\ &= a^4 + 4a^3 b + 6a^2 b^2 + 4ab^3 + b^4 \\ &= a^4 + 2a^2 b^2 + b^4 \\ &= (a^2 + b^2)^2\end{aligned}$$

page 182, #12: Let R be a commutative ring with unity of characteristic 3. Compute and simplify $(a + b)^9$ for all $a, b \in R$.

Since R is commutative, we can use the Binomial Theorem.

$$\begin{aligned}(a + b)^9 &= \sum_{k=0}^9 \binom{9}{k} a^{9-k} b^k \\ &= \binom{9}{0} a^9 + \binom{9}{1} a^8 b + \binom{9}{2} a^7 b^2 + \binom{9}{3} a^6 b^3 + \cdots + \binom{9}{9} b^9 \\ &= a^9 + 9a^8 b + 36a^7 b^2 + 84a^6 b^3 + 126a^5 b^4 + 126a^4 b^5 + 84a^3 b^6 + 36a^2 b^7 + 9ab^8 + b^9 \\ &= a^9 + b^9\end{aligned}$$

page 182, #30: This exercise shows that every ring R can be enlarged (if necessary) to a ring S with unity, having the same characteristic as R . Let $S = R \times \mathbb{Z}$ if R has characteristic 0, and $R \times \mathbb{Z}_n$ if R has characteristic n . Let addition in S be the usual addition by components, and let multiplication be defined by

$$(r_1, n_1)(r_2, n_2) = (r_1 r_2 + n_1 \cdot r_2 + n_2 \cdot r_1, n_1 n_2)$$

where $n \cdot r$ has the meaning explained in Section 18.

- a. Show that S is a ring.

S is an abelian group under addition, since it is the direct product of two abelian groups.

S is closed under multiplication by construction. Multiplication is associative by a long and exceedingly tedious computation:

$$\begin{aligned} ((r_1, n_1)(r_2, n_2))(r_3, n_3) &= (r_1r_2 + n_1 \cdot r_2 + n_2 \cdot r_1, n_1n_2)(r_3, n_3) \\ &= (r_1r_2r_3 + n_1 \cdot r_2r_3 + n_2 \cdot r_1r_3 + (n_1n_2) \cdot r_3 + n_3 \cdot r_1r_2 + (n_1n_3) \cdot r_2 + (n_2n_3) \cdot r_1, n_1n_2n_3) \\ (r_1, n_1)((r_2, n_2)(r_3, n_3)) &= (r_1, n_1)(r_2r_3 + n_2 \cdot r_3 + n_3 \cdot r_2, n_2n_3) \\ &= (r_1r_2r_3 + n_2 \cdot r_1r_3 + n_3 \cdot r_1r_2 + n_1 \cdot r_2r_3 + (n_1n_2) \cdot r_3 + (n_1n_3) \cdot r_2 + (n_2n_3) \cdot r_1, n_1n_2n_3) \\ &= ((r_1, n_1)(r_2, n_2))(r_3, n_3) \end{aligned}$$

A similarly long and tedious computation proves that the distributive laws hold, using the fact that they hold for R , \mathbb{Z} , and \mathbb{Z}_n .

$$\begin{aligned} (r_1, n_1)((r_2, n_2) + (r_3, n_3)) &= (r_1, n_1)(r_2 + r_3, n_2 + n_3) \\ &= (r_1r_2 + r_1r_3 + n_1 \cdot r_2 + n_1 \cdot r_3 + n_2 \cdot r_1 + n_3 \cdot r_1, n_1n_2 + n_1n_3) \\ (r_1, n_1)(r_2, n_2) + (r_1, n_1)(r_3, n_3) &= (r_1r_2 + n_1 \cdot r_2 + n_2 \cdot r_1, n_1n_2) + (r_1r_3 + n_1 \cdot r_3 + n_3 \cdot r_1, n_1n_3) \\ &= (r_1r_2 + n_1 \cdot r_2 + n_2 \cdot r_1 + r_1r_3 + n_1 \cdot r_3 + n_3 \cdot r_1, n_1n_2 + n_1n_3) \\ &= (r_1, n_1)((r_2, n_2) + (r_3, n_3)) \end{aligned}$$

and S is a ring.

- b. Show that S has unity.

Let 0_R be the additive identity for R , and 1 be the multiplicative identity for whichever of \mathbb{Z} and \mathbb{Z}_n is used. Then $(0_R, 1)$ is the unity for S .

$$\begin{aligned} (0_R, 1)(r, n) &= (0_Rr + 1 \cdot r + n \cdot 0_R, 1n) \\ &= (r, n) \end{aligned}$$

- c. Show that S and R have the same characteristic.

For the case where the characteristic of R is 0 , there is no non-zero integer n such that $n \cdot r = 0$. Then there is no such n with $n \cdot (r, m) = (n \cdot r, nm) = (0, 0)$, and S is also of characteristic 0 .

If the characteristic of R is n , then $n \cdot (r, m) = (n \cdot r, nm) = (0, 0)$, and no smaller positive integer will send r to 0 , so n is the characteristic of S as well.

- d. Show that the map $\phi: R \rightarrow S$ given by $\phi(r) = (r, 0)$ for $r \in R$ maps R isomorphically onto a subring of S .

ϕ sends sums to sums: $\phi(r_1 + r_2) = (r_1 + r_2, 0) = (r_1, 0) + (r_2, 0)$.

ϕ sends products to products: $\phi(r_1r_2) = (r_1r_2, 0) = (r_1r_2 + 0 \cdot r_2 + 0 \cdot r_2, 0 \cdot 0) = (r_1, 0)(r_2, 0)$.

ϕ is one-to-one: $\phi(r_1) = \phi(r_2)$ means that $(r_1, 0) = (r_2, 0)$ and $r_1 = r_2$.

By definition, a function maps onto its image. ϕ is an isomorphism onto its image, $\phi[R] = \{(r, 0) \mid r \in R\}$, which is a subring since it is an abelian group under addition, closed under multiplication, which is associative, and satisfies the distributive laws (since R does).

page 189, #17, 18: Describe all solutions of the given congruence, as we did in Examples 20.14 and 20.15.

page 189, #17: $155x = 75 \pmod{65}$

The gcd of 155 and 65 is 5. Since 5 divides into 75, we divide the congruence by 5 and solve it modulo $65/5 = 13$.

$$31x \equiv 25 \pmod{13}$$

$$\begin{aligned}
 5x &\equiv 12 \pmod{13} \\
 8(5x) &\equiv 8(12) \pmod{13} \\
 40x &\equiv 96 \pmod{13} \\
 x &\equiv 5 \pmod{13} \\
 x &\equiv 5, 18, 31, 44, 57 \pmod{65}
 \end{aligned}$$

page! 189, #18: $39x \equiv 52 \pmod{130}$

The gcd of 39 and 130 is 13. Since 13 divides into 52, we divide the congruence by 13 and solve it modulo $130/13 = 10$.

$$\begin{aligned}
 3x &\equiv 4 \pmod{10} \\
 7(3x) &\equiv 7(4) \pmod{10} \\
 21x &\equiv 28 \pmod{10} \\
 x &\equiv 8 \pmod{10} \\
 x &\equiv 8, 18, 28, 38, 48, 58, 68, 78, 88, 98, 108, 118, 128 \pmod{130}
 \end{aligned}$$

page 196, #1: Describe the field F of quotients of the integral subdomain

$$D = \{n + mi \mid n, m \in \mathbb{Z}\}$$

of \mathbb{C} . “Describe” means give the elements of \mathbb{C} that make up the field of quotients of D in \mathbb{C} . (The elements of D are the **Gaussian integers**.)

F consists of the numbers of the form $p + qi$ where $p, q \in \mathbb{Q}$. Any such number can be written over a common integer denominator, and thus expressed as a fraction of elements of D . Conversely, by rationalizing the denominator, we can express any such quotient as a number of the form $p + qi$.

page 196, #2: Describe (in the sense of Exercise 1) the field F of quotients of the integral subdomain $D = \{n + m\sqrt{2} \mid n, m \in \mathbb{Z}\}$ of \mathbb{R} .

The field F is (by similar reasoning) the numbers of the form $p + q\sqrt{2}$ where $p, q \in \mathbb{Q}$.