Algebra I Homework Five

Name:

Instruction: In the following questions, you should work out the solutions in a clear and concise manner. Three questions will be randomly selected and checked for correctness; they count 50% grades of this homework set. The other questions will be checked for completeness; they count the rest 50% grades of the homework set. Staple this page as the cover sheet of your homework set.

1. (Section 3.1) A ring R such that $a^2 = a$ for all $a \in R$ is called a Boolean ring. Prove that every Boolean ring R is commutative and $a + a = 0$ for all $a \in R$.

   For $a \in R$,
   $$a + a = (a + a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a \quad \Longrightarrow \quad a + a = 0.$$
   For $a, b \in R$,
   $$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b \quad \Longrightarrow \quad 0 = ab + ba = ab + ab \quad \Longrightarrow \quad ab = ba.$$

2. (Section 3.1) An element of a ring R is nilpotent if $a^n = 0$ for some n. Prove that in a commutative ring $a + b$ is nilpotent if a and b are. Show that this result may be false if R is not commutative.

   If a and b are nilpotent in a commutative ring R, then $a^n = b^m = 0$ for some $n, m \in \mathbf{N}$. Then
   $$\begin{aligned}
   (a+b)^{n+m-1} &= \sum_{i=0}^{n+m-1} \binom{n+m-1}{i} a^i b^{n+m-1-i} \\
   &= \sum_{j=0}^{n-1} \binom{n+m-1}{j} a^j b^{n+m-1-j} + \sum_{k=n}^{n+m-1} \binom{n+m-1}{k} a^k b^{n+m-1-k} \\
   &= \sum_{j=0}^{n-1} \binom{n+m-1}{j} a^j \cdot 0 + \sum_{k=n}^{n+m-1} \binom{n+m-1}{k} 0 \cdot b^{n+m-1-k} \\
   &= 0.
   \end{aligned}$$
   Hence $a + b$ is nilpotent.

   The result may be false if R is not commutative. For example, let $R = M_2(\mathbf{C})$, let $a = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ and $b = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Then a and b are nilpotent, however, $a + b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ is not nilpotent.

3. (Section 3.2) The ring E of even integers contains a maximal ideal M such that E/M is nor a field.

   $M = 4\mathbf{Z}$ is a maximal ideal of $E = 2\mathbf{Z}$ as no other ideals lying between $4\mathbf{Z}$ and $2\mathbf{Z}$. However, $E/M = \{M, 2+M\}$ where $(2 + M)^2 = 4 + M = M = (2 + M)M$. So E/M is not a field.

4. (Section 3.2) Determine all prime and maximal ideals in the ring $\mathbf{Z}_m$.

   The ideals of $\mathbf{Z}_m$ are of the form $(a) = a\mathbf{Z}_m$ for some factor a of m, whence the quotient ring $\mathbf{Z}_m/(a) \simeq \mathbf{Z}_a$.
   Let $p_1, \cdots, p_k$ be all the distinct prime factors of m. An ideal (a) of $\mathbf{Z}_m$ is prime [resp. maximal] iff $\mathbf{Z}_m/(a)$ is an integral domain [resp. field]. In either case, $a = p_i$ for $i = 1, \cdots, k$. Therefore, the prime ideals and maximal ideals in $\mathbf{Z}_m$ coincide and they are:
   $$(p_i) = p_i\mathbf{Z}_m, \qquad i = 1, \cdots, k.$$

5. (Section 3.2) If $R = \mathbf{Z}$, $A_1 = (6)$ and $A_2 = (4)$, then the ring homomorphism $\theta : R/(A_1 \cap A_2) \to R/A_1 \times R/A_2$ defined by $r + (A_1 \cap A_2) \mapsto (r + A_1, r + A_2)$ is not surjective.

   $(A_1, 1 + A_2) = (0 + (4), 1 + (6))$ is not the θ-image of any $r + A_1 \cap A_2 = r + (12)$ for $r \in \mathbf{Z}$. This shows that θ is not surjective.

6. (Section 3.3) Let R be the subring $\{a + b\sqrt{10} \mid a, b \in \mathbf{Z}\}$ of the field of real numbers.

   (a) The map $N : R \to \mathbf{Z}$ given by $a + b\sqrt{10} \mapsto (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2$ is such that $N(uv) = N(u)N(v)$ for all $u, v \in R$ and $N(u) = 0$ if and only if $u = 0$.

   For any $u = a_1 + b_1\sqrt{10},\ v = a_2 + b_2\sqrt{10} \in R$,

$$\begin{aligned} N(uv) &= (a_1 + b_1\sqrt{10})(a_2 + b_2\sqrt{10})(a_1 - b_1\sqrt{10})(a_2 - b_2\sqrt{10}) \\ &= (a_1 + b_1\sqrt{10})(a_1 - b_1\sqrt{10})(a_2 + b_2\sqrt{10})(a_2 - b_2\sqrt{10}) = N(u)N(v). \end{aligned}$$

   If $N(u) = a_1^2 - 10b_1^2 = 0$, then $a_1^2 = 10b_1^2$. When $a_1 \neq 0$ or $b_1 \neq 0$, there are even number of factor 2 in a_1^2 but odd number of factor 2 in $10b_1^2$, which is impossible. Therefore, $a_1 = b_1 = 0$ and $u = 0$.

   (b) u is a unit in R if and only if $N(u) = \pm 1$.

   If u is a unit in R, then there is $v \in R$ such that $uv = 1$. Then $N(u)N(v) = N(uv) = N(1) = 1$. So $N(u) = \pm 1$.

   Conversely, if $N(u) = \pm 1$ for $u = a + b\sqrt{10} \in R$, let $v = \pm(a - b\sqrt{10}) \in R$ then $uv = \pm(a^2 - 10b^2) = \pm N(u) = 1$. So u is a unit in R.

   (c) $2, 3, 4 + \sqrt{10}$ and $4 - \sqrt{10}$ are irreducible elements of R.

   If 2 is not irreducible, then $2 = uv$ where u and v are nonzero nonunits in R. Then $4 = N(2) = N(u)N(v)$. By the preceding argument, $N(u) = N(v) = \pm 2$ since u and v are not units. Suppose $u = a + b\sqrt{10}$. If $N(u) = 2$, then $a^2 - 10b^2 = 2$ and thus $a^2 \equiv 2 \mod 10$. However, this is impossible. Likewise, it is impossible for $N(u) = -2$. Therefore, 2 must be irreducible.

   Similar arguments show that 3, $4 + \sqrt{10}$ and $4 - \sqrt{10}$ are irreducible.

   (d) $2, 3, 4 + \sqrt{10}$ and $4 - \sqrt{10}$ are not prime elements of R. [Hint: $3 \cdot 2 = 6 = (4 + \sqrt{10})(4 - \sqrt{10})$.]

   We have $3 \cdot 2 = 6 = (4 + \sqrt{10})(4 - \sqrt{10})$ in R. If 2 is a prime element of R, then 2 divides one of $4 + \sqrt{10}$ or $4 - \sqrt{10}$ in R. It implies that $N(2) = 4$ divides $N(4 + \sqrt{10}) = 6$ or $N(4 - \sqrt{10}) = 6$ in $\mathbf{Z}$. This is a contradiction. Hence 2 is not a prime element of R.

   Similar arguments show that 3, $4 + \sqrt{10}$ and $4 - \sqrt{10}$ are not prime elements of R.

7. (Section 3.3) If R is a unique factorization domain and $a, b \in R$ are relatively prime and $a \mid bc$, then $a \mid c$.

   The assumption $a \mid bc$ implies that $ad = bc$ for certain $d \in R$. Suppose that a, b, c and d are factorized into products of irreducible elements as follow:

$$a = \prod_{i=1}^{\ell} a_i, \qquad b = \prod_{j=1}^{m} b_j, \qquad c = \prod_{k=1}^{n} c_k, \qquad d = \prod_{r=1}^{s} d_r,$$

   where a_i, b_j, c_k, d_r are irreducible in R. Then

$$\left(\prod_{i=1}^{\ell} a_i\right)\left(\prod_{r=1}^{s} d_r\right) = \left(\prod_{j=1}^{m} b_j\right)\left(\prod_{k=1}^{n} c_k\right).$$

   The unique factorization property means that $\ell + s = m + n$ and that there is a one-to-one correspondence between $\{a_1, \cdots, a_\ell, d_1, \cdots, d_s\}$ and $\{b_1, \cdots, b_m, c_1, \cdots, c_n\}$, where the corresponding elements are associates. Each a_i could not be associate to a b_j, since otherwise $a_i \mid \gcd(a, b)$, which contradicts the assumption that a and b are relatively prime. Therefore, each a_i associates to certain c_k. Hence $a \mid c$.

8. (Section 3.3) Every nonempty set of elements (possibly infinite) in a commutative principal ideal ring with identity has a greatest common divisor.

   Let X be a nonempty set of elements in a commutative principal ideal ring R with identity. Then $(X) = \sum_{x \in X}(x) = (a)$ for some $a \in R$. We claim that a is a gcd of X. On one hand, for $x \in X$, we have $(x) \subseteq (X) = (a)$. Thus $a \mid x$. On the other hand, if $y \mid x$ for every $x \in X$, then $(y) \supseteq (x)$ for all $x \in X$. Thus $(y) \supseteq (X) = (a)$, which implies that $y \mid a$. Therefore, a is a gcd of X.

9. (Section 3.6)

(a) If D is an integral domain which contains at least one irreducible element, then $D[x]$ is not a principal ideal domain. [Hint: suppose c is an irreducible element in D. Consider the ideal (x, c).]

Suppose c is an irreducible element in D. Consider the ideal (x, c). If $(x, c) = (d)$ for some $d \in D$, then $c = dk$ for some $k \in D$. Since c is irreducible, either d is a unit or k is a unit. If d is a unit, then $(x, c) = (1_R) = R$, which is impossible since $(x, c) = cR + xR$ does not contain 1_R. If k is a unit, then c and d are associates and $(x, c) = (d) = (c)$, a contradiction since $x \notin (c)$. The argument shows that (x, c) is not a principal ideal, and thus $D[x]$ is not a princial ideal domain.

(b) $\mathbf{Z}[x]$ is not a principal ideal domain.

$\mathbf{Z}$ has an irreducible element 2.

(c) If F is a field and $n \geq 2$, then $F[x_1, \cdots, x_n]$ is not a principal ideal domain. [Hint: show that x_1 is irreducible in $F[x_1, \cdots, x_{n-1}]$.]

x_1 is irreducible in $F[x_1, \cdots, x_{n-1}]$. Therefore, $F[x_1, \cdots, x_{n-1}, x_n] = F[x_1, \cdots, x_{n-1}][x_n]$ is not a principal ideal domain, as (x_1, x_n) is not a principal ideal.

10. (Section 3.6) If F is a field, then x and y are relatively prime in the polynomial domain $F[x, y]$, but $F[x, y] = (1_F) \underset{\neq}{\supset} (x) + (y)$ [compare Theorem 3.11 (i)].

The ideal $(x) + (y) = (x, y)$ is not a principal ideal by the preceding question. If z is a gcd of x and y, then $z \mid x$ implies that $(z) \supseteq (x)$. Similarly $(z) \supseteq (y)$. Therefore, $(z) \supsetneq (x, y)$.

Let $f \in F[x, y]$ be any divisor of x and y. Then $\deg f \leq \deg x = 1$. So $f = a + bx + cy$ for some $a, b, c \in F$. By direct computation, $b = c = 0$, and a must be a unit. Therefore, 1_F is a gcd of x and y.