Honors Algebra 4, MATH 371 Winter 2010

Solutions 2

1. Let R be a ring.

   (a) Let I be an ideal of R and denote by $\pi : R \to R/I$ the natural ring homomorphism defined by $\pi(x) := x \bmod I$ $(= x + I$ using coset notation). Show that an arbitrary ring homomorphism $\phi : R \to S$ can be factored as $\phi = \psi \circ \pi$ for some ring homomorphism $\psi : R/I \to S$ if and only if $I \subseteq \ker(\phi)$, in which case ψ is unique.

   (b) Suppose that R is commutative with 1. An R-*algebra* is a ring S with identity equipped with a ring homomorphism $\phi : R \to S$ mapping 1_R to 1_S such that $\mathrm{im}(\phi)$ is contained in the center of S (*i.e.* the set

   $$c(S) := \{z \in S \mid zs = sz \text{ for all } s \in S\}$$

   of all elements of S that commute with every other element). If (S, ϕ) and (S', ϕ') are two R-algebras then a ring homomorphism $f : S \to S'$ is called a *homomorphism of R-algebras* if $f(1_S) = 1_{S'}$ and $f \circ \phi = \phi'$. For an R-algebra (S, ϕ) we will frequently simply write rx for $\phi(r)x$ whenever $r \in R$ and $x \in S$.

   Prove that the polynomial ring $R[X]$ in one variable is naturally an R-algebra, and that if S is an R-algebra then for any $s \in S$ there exists a unique R-algebra homomorphism $f : R[X] \to S$ such that $f(X) = s$. In other words, mapping $R[X]$ to S is the "same" as choosing an element s of S.

   Solution:

   (a) One direction is obvious. For the other direction, assume that $I \subseteq \ker(\phi)$ and define $\psi : R/I \to S$ by the rule

   $$\psi(r + I) := \phi(r).$$

   Note that this is well-defined since it doesn't depend on the choice of coset representative as $\phi(I) = 0$. Clearly $\phi = \psi \circ \pi$ and if $\psi' : R/I \to S$ is another ring map with this property then we must have $\psi = \psi'$ as π is surjective. Hence ψ is unique.

   (b) That $R[X]$ is an R-algebra via the map $R \to R[X]$ sending $r \in R$ to the constant polynomial $r \in R[X]$ is obvious. If S is any R-algebra and $s \in S$, we define $f : R[X] \to S$ as

   $$f(a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n) := a_0 + a_1 s + \cdots a_n s^n.$$

   It is easy to check that f is an R-algebra homomorphism. On the other hand, if $f : R[X] \to S$ is any homomorphism of R-algebras with $f(X) = s$ then we must have $f(X^n) = f(X)^n = s^n$ and hence

   $$f(a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n) = f(a_0) + f(a_1)s + \cdots + f(a_n)s^n = a_0 + a_1 s + \cdots a_n s^n.$$

We conclude that f exists and is uniquely determined by the requirement that $f(X) = s$.

2. Let R be a ring with 1.

   (a) Prove that there is a unique map of rings $f_R : \mathbf{Z} \to R$. Conclude that every ring with 1 is a $\mathbf{Z}$-algebra in a unique way.

   (b) For a ring R with 1, the kernel of the ring homomorphism f_R as in (2a) is an ideal of $\mathbf{Z}$ so it has the form $c(R)\mathbf{Z}$ for a unique $c(R) \in \mathbf{Z}$ satisfying $c(R) \geq 0$. By definition, the *characteristic of* R is this integer $c(R)$. Convince yourself that when $c(R) > 0$, this number is the least number of times we have to add $1 \in R$ to itself to get $0 \in R$. Now prove that if R is a ring with 1 that is an integral domain, then the characteristic of R is either 0 or a prime number.

   (c) Prove that for $g : R \to S$ a homomorphism of rings with 1 taking 1_R to 1_S the characteristic of S divides the characteristic of R.

   (d) Let $g : R \to S$ be a homomorphism of rings with 1 taking 1_R to 1_S. If g is injective, prove that $c(R) = c(S)$. Give an example with g not injective where $c(R) \neq c(S)$.

Solution:

(a) In general, one wants maps of rings with 1 to take 1 to 1, but I should have explicitly demanded this. In this situation, for $n > 0$

$$f(n) = f(1) + f(n-1) = 1 + f(n-1)$$

and it follows by induction that $f(n)$ for $n > 0$ is uniquely determined. Using the existence of additive inverses in R, we must have $f(0) = 0$ as $f(0) = f(0+0) = f(0) + f(0)$. We conclude that for $n > 0$ we have

$$0 = f(0) = f(n + (-n)) = f(n) + f(-n)$$

and hence that $f(-n) = -f(n)$ is again uniquely determined. Thus, there is a unique map of rings $\mathbf{Z} \to R$ (provided we require 1 maps to 1).

(b) In any case, we have an injective homomorphism of rings

$$\mathbf{Z}/c(R)\mathbf{Z} \hookrightarrow R.$$

If R is a domain then so is $\mathbf{Z}/c(R)\mathbf{Z}$ since any subring of a domain is a domain and it follows that $(c(R))$ must be a prime ideal. Hence either $c(R) = 0$ or it is a prime number.

(c) The composite homomorphism

$$\mathbf{Z} \xrightarrow{f_R} R \longrightarrow S$$

coincides with f_S by uniqueness and hence $\ker(f_R) \subseteq \ker(f_S)$ as desired.

(d) When $g : R \to S$ is injective, the composite

$$\mathbf{Z}/c(R)\mathbf{Z} \xhookrightarrow{f_R} R \hookrightarrow S$$

is also injective and we deduce that $c(S) := \ker(f_S) = c(R)$. As a counterexample to this equality when g fails to be injective, consider the quotient map $\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$.

3. Let I and J be ideals of a ring R. We define

   (a) $I + J := \{a + b \mid a \in I,\ b \in J\}$
   (b) $IJ := \{a_1 b_1 + \cdots + a_s b_s \mid a \in I,\ b \in J\}$

   Prove that $I+J$ is the smallest ideal of R containing I and J and that IJ is an ideal contained in the intersection $I \cap J$. Convince yourself that $I \cap J$ is an ideal of R, and show that if R is commutative and $I + J = R$ then $IJ = I \cap J$. Show by giving examples that $IJ \neq I \cap J$ in general, and that $I \cup J$ (set-theoretic union) need not be an ideal.

   Solution: It is easy to see that $I + J$ is an ideal of R. If K is any ideal of R containing I and J then it contains a for all $a \in I$ and b for all $b \in J$ and hence $a + b$. Thus, K contains $I + J$.

   We obviously have $IJ \subseteq I \cap J$. To get the reverse inclusion, we have to require that $1 \in R$ (this should have been stated as an assumption in the problem). Suppose that $r \in I \cap J$ and write $1 = i + j$ for $i \in I$ and $j \in J$. Then $r = ri + rj$ lies in IJ. As for counterexamples, consider the ring $R = 2\mathbf{Z}$ which does not have an identity and the ideals $I = 6\mathbf{Z}$ and $J = 8\mathbf{Z}$. These ideals clearly satisfy $I + J = R$. We have $I \cap J = 24\mathbf{Z}$ but $IJ = 48\mathbf{Z}$. Now consider $2\mathbf{Z}$ and $3\mathbf{Z}$ as ideals of $\mathbf{Z}$. Their set-theoretic union contains 2 and 3 but not $2 + 3 = 5$ since 5 isn't a $\mathbf{Z}$-multiple of either 2 or 3.

4. Let R be a commutative ring and I, J ideals of R. If P is a prime ideal of R containing IJ, prove that P contains I or P contains J.

   Solution: Suppose that P does not contain I and let $j \in J$ be arbitrary. Since P does not contain I, there exists $i \in I$ with $i \notin P$. But $ij \in P$ whence $j \in P$ as P is prime. Hence P contains J.

5. Let R be a commutative ring.

   (a) Show that the set of all nilpotent elements of R (called the *nilradical of* R) is an ideal. Hint: this is basically 1(b) from assignment 1, but be careful about showing that this set is really an abelian group under addition.
   (b) Prove that the nilradical of R is contained in the intersection of all prime ideals of R.

(c) Let $G := \mathbf{Z}/p\mathbf{Z}$ as a group under addition (it is cyclic of order p). Let $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$ as a ring, and note that this is a field with p elements. Let R be the group ring $R := \mathbf{F}_p G$. What is the nilradical of R?

Solution:

(a) Using assignment 1, it remains to show that if x is nilpotent then so is $-x$. Note that for any $r \in R$ we have

$$0 = 0 \cdot r = (x + (-x))r = xr + (-x)r$$

so $(-x)r = -xr$. We deduce that

$$(-x)^n = \begin{cases} x^n & n \in 2\mathbf{Z} \\ -x^n & \text{else} \end{cases}$$

and hence that $-x$ is nilpotent of x is. Note that we don't need to assume that R has an identity.

(b) If $x \in R$ satisfies $x^n = 0$ for $n > 1$ and P is a prime ideal then $x^n = x \cdot x^{n-1} \in P$ so by induction $x \in P$. It follows that x lies in the intersection of all prime ideals.

(c) Arguing as in assignment 1, we have an isomorphism of rings

$$\mathbf{F}_p[X]/(x^p - 1) = \mathbf{F}_p G.$$

But as polynomials over $\mathbf{F}_p$ we have $x^p - 1 = (x-1)^p$ so our task is to find the nilradical of $\mathbf{F}_p[X]/(x-1)^p$. In other words, we seek to find all $f \in \mathbf{F}_p[X]$ such that $f^k \in (x-1)^p$ for some k. Since $(x-1)$ is a prime ideal of $\mathbf{F}_p[X]$, we conclude that we must have $f \in (x-1)^i$ for some $i \geq 1$ and hence the nilradical is precisely the principal ideal generated by $(x-1)$.

6. Let R be a commutative ring. Prove that the set of prime ideals in R has minimal elements with respect to inclusion. Such minimal elements are called *minimal primes*.

Solution: This exercise should require R to have an identity $1 \neq 0$. Let S be the set of prime ideals of R, ordered by inclusion. Since R is not the zero ring, R has at least one maximal (hence prime) ideal so S is nonempty. Suppose that I is any totally ordered set and that $\{P_i\}_{i \in I}$ is a chain in S. We claim that

$$P := \bigcap_{i \in I} P_i$$

is a prime ideal of R. It is clearly an ideal, so suppose that $ab \in P$. Then for all i, either $a \in P_i$ or $b \in P_i$. If $a \notin P_i$ for some $i \in I$, then $a \notin P_j$ for all $j \leq i$ as $P_j \subseteq P_i$ and hence

$b \in P_j$ for all $j \leq i$. As we must also then have $b \in P_j$ for all $j \geq i$ we deduce that $b \in P$ and P is prime. Thus, every chain in S is bounded below and we conclude by Zorn's Lemma (in the form with minimal elements) that S has minimal elements, as desired.

7. Let R be a finite (as a set) commutative ring with 1. Prove that every prime ideal of R is maximal.

   Solution: Let P be a prime ideal of R. Then R/P is a domain with finitely many elements, and is hence a field. (Indeed, if $x \in R/P$ is nonzero then the powers of x can not all be distinct by finiteness so $x^j = x^j$ for some $0 < i < j$ and we conclude that $x^{j-i}(x^i - 1) = 0$ so since R/P is a domain and $x \neq 0$ we conclude that $x^i = 1$ for some $i \geq 1$ whence x is a unit.) We conclude that P is maximal, as desired.

8. Let $\varphi : R \to S$ be a homomorphism of commutative rings and I an ideal of S. Prove that $\varphi^{-1}(I)$ (set-theoretic inverse image) is an ideal of R that is prime whenever I is a prime ideal of S. Show that this holds with "prime" replaced by "maximal" provided we assume that φ is surjective. Give a counterexample to this if we drop the surjectivity requirement.

   Solution: The map φ induces an injective homomorphism of rings

   $$R/\varphi^{-1}(I) \hookrightarrow S/I$$

   so if the target is a domain, so is the source as any subring of a domain is a domain. In the case that φ is surjective, this induced map is an isomorphism so if I is maximal both target and source are fields and $\varphi^{-1}(I)$ must be maximal as well. As a counterexample, consider the map $\mathbf{Z} \hookrightarrow \mathbf{Q}$ given by inclusion. The zero ideal of $\mathbf{Q}$ is maximal as $\mathbf{Q}$ is a field, but clearly its inverse image—the zero ideal of $\mathbf{Z}$—is not maximal.

   Suppose that $ab \in \varphi^{-1}(I)$. Then $\varphi(a)\varphi(b) \in I$ so if I is prime one of $\varphi(a), \varphi(b)$ lies in I and hence one of a, b lies in $\varphi^{-1}(I)$. If φ is surjective and I is maximal