Kris Harper
MATH 25800
Homework 1 January 15, 2010

Problem 1 (7.1.3)**.** *Let R be a ring with identity and let S be a subring of R containing the identity. Prove that if u is a unit in S then u is a unit in R. Show by example that the converse is false.*

Proof. Let u be a unit in S. Then there exists $v \in S$ such that $uv = 1$. But since S is a subring of R, $v \in R$ and so $uv = 1$ in R as well. Thus u is a unit in R as well. Conversely, the ring of integers has $2\mathbb{Z}$ as a subring, which has no units, while 1 and -1 are units in $\mathbb{Z}$. □

Problem 2 (7.1.5)**.** *Decide which of the following (a)-(f) are subrings of $\mathbb{Q}$:*
(a) The set of all rational numbers with odd denominators (when written in lowest terms).
(b) The set of all rational numbers with even denominators (when written in lowest terms).
(c) The set of nonnegative rational numbers.
(d) The set of squares of rational numbers.
(e) The set of all rational numbers with odd numerators (when written in lowest terms).
(f) The set of all rational numbers with even numerators (when written in lowest terms).

Proof. (a) This is a subring of $\mathbb{Q}$. Let a/b and c/d be elements of $\mathbb{Q}$ written in lowest terms with b and d odd. Then $a/b - c/d = (ad - bc)/bd$ and since b and d are both odd, bd is odd as well. It may be possible to reduce this fraction, but since there are no factors of 2 in bd, there can be no factors of 2 in the reduced form either. Likewise, $a/b \cdot c/d = ac/bd$ which is in our set for the same reasons as above. Since this set is closed under subtraction and multiplication, we must have a subring.

(b) This is also a subring of $\mathbb{Q}$. Now assume that b and d are even. We still have $a/b - c/d = (ad - bc)/bd$. In this case b and d are even, so bd is clearly even. Supposing that $(ad - bc)/bd$ doesn't have an even denominator when reduced, it must be the case that ad and bc each have as many factors of 2 as bd does. This means that a must have as many factors of 2 as b does. But then a/b wasn't in lowest terms to begin with. This is a contradiction, so $(ad - bc)/bd$ must have an even denominator. Likewise ac/bd must have an even denominator because otherwise a or c would have at least one factor of 2 shared with b or d respectively. Thus, this set is closed under subtraction and multiplication and must be a subring.

(c) These don't form a group under addition since no element has an additive inverse.

(d) These don't form a group under addition. For example, $1/4 = (1/2)^2$ and $1/4 + 1/4 = 1/2$. But we know $\sqrt{2}$ is irrational.

(e) These aren't closed under addition. For example, $1/3 + 1/3 = 2/3$.

(f) This is a subring of $\mathbb{Q}$. Let a/b and c/d be elements of $\mathbb{Q}$ with a and c even. Then $a/b - c/d = (ad - bc)/bd$. Since a and c are even they each contain a factor of 2 and so using the distributive law for integers, $ad - bc$ also contains a factor of 2 and is thus even. If we suppose that $(ad - bc)/bd$ reduces to a fraction with an odd numerator, then either b or d must contain a factor of 2. Without loss of generality, we can assume $2 \mid b$, but then a/b isn't in lowest terms. Therefore $(ad - bc)/bd$ reduces to a fraction with an even numerator so the set is closed under subtraction. Likewise, $a/b \cdot c/d = ac/bd$ and clearly ac is even. We arrive at the same contradiction as above if ac/bd reduces to a fraction with odd numerator. Thus our set is closed under multiplication and so must be a subring of $\mathbb{Q}$. □

Problem 3 (7.1.7)**.** *The center of ring R is $\{z \in R \mid zr = rz \text{ for all } r \in R\}$ (i.e., the set of all elements which commute with every element of R). Prove that the center of a ring is a subring that contains the identity. Prove that the center of a division ring is a field.*

Proof. Let R be a ring and let Z be the center of R. Clearly $1 \in Z$ since $1 \cdot r = r \cdot 1$ for all $r \in R$. Let $u, v \in Z$ and $r \in R$. Then $(uv)r = u(vr) = u(rv) = (ur)v = (ru)v = r(uv)$ so $uv \in Z$. Likewise $(u - v)r = ur - vr = ru - rv = r(u - v)$. Thus Z is closed under subtraction and multiplication so it must be a subring of R. If R is a division ring and $u \in Z$ then there exists $v \in R$ such that $uv = vu = 1$. Now for an arbitrary $r \in R$ consider $vr = vr(uv) = v(ru)v = v(ur)v = (vu)rv = rv$. Thus $v \in Z$ as well. This shows that Z is a division ring whenever R is a division ring. Since Z is clearly commutative, in this case we must have that Z is a field. □

Kris Harper
MATH 25800
Homework 1
January 15, 2010

Problem 4 (7.1.9)**.** *For a fixed element $a \in R$ define $C(a) = \{r \in R \mid ra = ar\}$. Prove that $C(a)$ is a subring of R containing a. Prove that the center of R is the intersection of the subrings $C(a)$ over all $a \in R$.*

Proof. Let $r, s \in C(a)$ for some $a \in R$. Then $(r-s)a = ra - sa = ar - as = a(r-s)$ and $(rs)a = r(sa) = r(as) = (ra)s = (ar)s = a(rs)$ so $C(a)$ is closed under subtraction and multiplication. Furthermore $a \in C(a)$ since $aa = aa$ and so $C(a)$ is a subring of R containing a. Let Z be the center of R. If $z \in Z$ then for a given $a \in R$ we have $za = az$ so $z \in C(a)$. Thus $Z \subseteq \bigcap_{a \in R} C(a)$. On the other hand, if $r \in \bigcap_{a \in R} C(a)$ then $ra = ar$ for all $a \in R$ so $r \in Z$. Both inclusions have been shown so we must have $Z = \bigcap_{a \in R} C(a)$. □

Problem 5 (7.1.15)**.** *A ring R is called a* Boolean ring *if $a^2 = a$ for all $a \in R$. Prove that every Boolean ring is commutative.*

Proof. Let R be a Boolean ring and let $a, b \in R$. Then

$$a + a = (a+a)^2 = a^2 + a + a + a^2 = a + a + a + a$$

so we have $a + a = 0$ or $a = -a$. This holds for all elements of R. But now,

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

and so $ab + ba = 0$ and using the above fact, $ab = ba$. □

Problem 6 (7.2.2)**.** *Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be an element of the polynomial ring $R[x]$. Prove that $p(x)$ is a zero divisor if and only if there is a nonzero $b \in R$ such that $bp(x) = 0$.*

Proof. Assume that $a_n \neq 0$, otherwise we may have $p(x) = 0$ which is not a zero divisor. If there exists nonzero $b \in R$ with $bp(x) = 0$ then clearly $p(x)$ is a zero divisor. To show the converse, let $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ be a nonzero polynomial of minimal degree such that $g(x)p(x) = 0$. Note that this implies the leading coefficient of $g(x)p(x)$, $b_m a_n = 0$. Thus $a_n g(x)$ is a polynomial of degree less than m such that $a_n g(x)p(x) = 0$. Since $g(x)$ is nonzero of minimal degree we must have $a_n g(x) = 0$. Now use induction on i and assume that $a_{n-i}g(x) = 0$ for some i. Then we must have $a_{n-i}b_{m-1} = 0$ which means $a_{n-i-1}b_m = 0$ as well. Therefore $a_{n-i-1}g(x)$ is a polynomial of degree less than m which has the property that $a_{n-i-1}g(x)p(x) = 0$. By the minimality of $g(x)$ we must have $a_{n-i-1}g(x) = 0$. Thus $a_{n-i}g(x) = 0$ for all $i = 0, 1, \ldots, n$ and hence $b_m p(x) = 0$. □

Problem 7 (7.2.4)**.** *Prove that if R is an integral domain then the ring of formal power series $R[[x]]$ is also an integral domain.*

Proof. Let $p(x) = \sum_{n=0}^{\infty} a_n x^n$ and $q(x) = \sum_{n=0}^{\infty} b_n x^n$ with $p(x)$ and $q(x)$ nonzero. Then

$$p(x)q(x) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_n b_{n-k} \right) x^n.$$

Since $p(x)$ and $q(x)$ are both nonzero, there exists some i and some j such that $a_i \neq 0$ and $b_j \neq 0$. But then then $(i+j)^{\text{th}}$ term in $p(x)q(x)$ will contain $a_i b_j$ and since R is an integral domain, this term is nonzero. Thus, any two nonzero elements of $R[[x]]$ have a nonzero product and so $R[[x]]$ has no zero divisors. It is therefore an integral domain. □

Problem 8 (7.2.10)**.** *Consider the following elements of the integral group ring $\mathbb{Z}S_3$:*

$$\alpha = 3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3) \quad \textit{and} \quad \beta = 6(1) + 2(2\ 3) - 7(1\ 3\ 2)$$

(where (1) is the identity of S_3). Compute the following elements:
(a) $\alpha + \beta$,
(b) $2\alpha - 3\beta$,
(c) $\alpha\beta$,
(d) $\beta\alpha$,
(e) α^2.

Kris Harper
MATH 25800
Homework 1 January 15, 2010

Proof. (a) $\alpha + \beta = 6(1) + 3(1\ 2) - 3(2\ 3) + 14(1\ 2\ 3) - 7(1\ 3\ 2)$.

(b)

$$\begin{aligned} 2\alpha - 3\beta &= 2(3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3)) - 3(6(1) + 2(2\ 3) - 7(1\ 3\ 2)) \\ &= 6(1\ 2) - 10(2\ 3) + 28(1\ 2\ 3) - 18(1) - 6(2\ 3) + 21(1\ 3\ 2) \\ &= -18(1) + 6(1\ 2) - 16(2\ 3) + 28(1\ 2\ 3) + 21(1\ 3\ 2) \end{aligned}$$

(c)

$$\begin{aligned} \alpha\beta &= (3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3))(6(1) + 2(2\ 3) - 7(1\ 3\ 2)) \\ &= 3(1\ 2)(6(1) + 2(2\ 3) - 7(1\ 3\ 2)) - 5(2\ 3)(6(1) + 2(2\ 3) - 7(1\ 3\ 2)) + 14(1\ 2\ 3)(6(1) + 2(2\ 3) - 7(1\ 3\ 2)) \\ &= 18(1\ 2) + 6(1\ 2)(2\ 3) - 21(1\ 2)(1\ 3\ 2) - 30(2\ 3) - 10(2\ 3)(2\ 3) \\ &+ 35(2\ 3)(1\ 3\ 2) + 84(1\ 2\ 3) + 28(1\ 2\ 3)(2\ 3) - 98(1\ 2\ 3)(1\ 3\ 2) \\ &= 18(1\ 2) + 6(1\ 2\ 3) - 21(1\ 3) - 30(2\ 3) - 10(1) + 35(1\ 2) + 84(1\ 2\ 3) + 28(1\ 2) - 98(1) \\ &= 81(1\ 2) + 90(1\ 2\ 3) - 21(1\ 3) - 30(2\ 3) - 108(1). \end{aligned}$$

(d)

$$\begin{aligned} \beta\alpha &= (6(1) + 2(2\ 3) - 7(1\ 3\ 2))(3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3)) \\ &= 6(1)(3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3)) + 2(2\ 3)(3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3)) - 7(1\ 3\ 2)(3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3)) \\ &= 18(1\ 2) - 30(2\ 3) + 84(1\ 2\ 3) + 6(2\ 3)(1\ 2) - 10(2\ 3)(2\ 3) + 28(2\ 3)(1\ 2\ 3) \\ &- 21(1\ 3\ 2)(1\ 2) + 35(1\ 3\ 2)(2\ 3) - 98(1\ 3\ 2)(1\ 2\ 3) \\ &= 18(1\ 2) - 30(2\ 3) + 84(1\ 2\ 3) + 6(1\ 3\ 2) - 10(1) + 28(1\ 3) - 21(2\ 3) + 35(1\ 3) - 98(1) \\ &= 18(1\ 2) - 51(2\ 3) + 84(1\ 2\ 3) + 6(1\ 3\ 2) - 108(1) + 63(1\ 3). \end{aligned}$$

(e)

$$\begin{aligned} \alpha^2 &= (3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3))(3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3)) \\ &= 3(1\ 2)(3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3)) - 5(2\ 3)(3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3)) + 14(1\ 2\ 3)(3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3)) \\ &= 9(1\ 2)(1\ 2) - 15(1\ 2)(2\ 3) + 42(1\ 2)(1\ 2\ 3) - 15(2\ 3)(1\ 2) + 25(2\ 3)(2\ 3) \\ &- 70(2\ 3)(1\ 2\ 3) + 42(1\ 2\ 3)(1\ 2) - 70(1\ 2\ 3)(2\ 3) + 196(1\ 2\ 3)(1\ 2\ 3) \\ &= 9(1) - 15(1\ 2\ 3) + 42(2\ 3) - 15(1\ 3\ 2) + 25(1) - 70(1\ 3) + 42(1\ 3) - 70(1\ 2) + 196(1\ 3\ 2) \\ &= 34(1) - 15(1\ 2\ 3) + 42(2\ 3) + 181(1\ 3\ 2) + 28(1\ 3) - 70(1\ 2). \end{aligned}$$

□

Problem 9 (7.2.13)**.** *Let $\mathcal{K} = \{k_1, \ldots, k_m\}$ be a conjugacy class in the finite group G.*
(a) Prove that the element $K = k_1 + \cdots + k_m$ is in the center of the group ring RG.
(b) Let $\mathcal{K}_1, \ldots, \mathcal{K}_r$ be the conjugacy classes of G and for each $\mathcal{K}_i$ let K_i be the element of RG that is the sum of the members of $\mathcal{K}_i$. Prove that an element $\alpha \in RG$ is in the center of RG if and only if $\alpha = a_1K_1 + a_2K_2 + \cdots + a_rK_r$ for some $a_1, a_2, \ldots, a_r \in R$.

Proof. (a) Let $r \in RG$ and let Z be the center of RG. Note that since $\mathcal{K}$ is a conjugacy class and G is finite, if $g \in G$ then for each i, $g^{-1}k_ig = k_j$ for some j. Furthermore this is an injective map and so $g^{-1}Kg = K$.

Now suppose $r = r_1g_1 + \cdots + r_ng_n$ so that

$$\begin{aligned} rK &= (r_1g_1 + \cdots + r_ng_n)K \\ &= r_1g_1K + \cdots + r_ng_nK \\ &= r_1g_1(g_1^{-1}Kg_1) + \cdots + r_ng_n(g_n^{-1}Kg_n) \\ &= r_1Kg_1 + \cdots + r_nKg_n \\ &= Kr_1g_1 + \cdots + Kr_ng_n \\ &= K(r_1g_1 + \cdots + r_ng_n). \end{aligned}$$

Thus $K \in Z$.

(b) Let $u = r_1g_1 + \cdots + r_ng_n$ be an element of RG and let $\alpha = a_1K_1 + \cdots + a_rK_r$. Now using part (a) and the fact that R is commutative we have

$$\alpha u = (a_1K_1 + \cdots + a_rK_r)u = a_1K_1u + \cdots + a_rK_ru = a_1uK_1 + \cdots + a_ruK_r = ua_1K_1 + \cdots + ua_rK_r = u\alpha.$$

Conversely, let α be in the center of RG. Suppose to the contrary that α doesn't contain the terms a_iK_i for some i. Then choose an element from $\mathcal{K}_i$ which does appear in α, say k_x and one that doesn't, say k_y. Note that there must exist g such that $gk_xg^{-1} = k_y$. But since α is in the center of RG we also have $g\alpha g^{-1} = \alpha$. By supposition α has the term rk_x for some $r \in RG$, yet this means $g\alpha g^{-1}$ contains the term rk_y. This is a contradiction and so α must contain all members of each conjugacy class with matching coefficients from R. □

Problem 10 (7.3.10)**.** *Decide which of the following are ideals of the ring $\mathbb{Z}[x]$:*
(a) The set of all polynomials whose constant term is a multiple of 3.
(b) The set of all polynomials whose coefficient of x^2 is a multiple of 3.
(c) The set of all polynomials whose constant term, coefficient of x and coefficient of x^2 are zero.
(d) $\mathbb{Z}[x^2]$ (i.e., the polynomials in which only even powers of x appear.
(e) The set of all polynomials whose coefficients sum to zero.
(f) The set of polynomials $p(x)$ such that $p'(0) = 0$, where $p'(x)$ is the usual first derivative of $p(x)$ with respect to x.

Proof. (a) Two integers which are multiples of 3 have a difference and product which is also a multiple of 3. Since this set is also nonempty, we see that it must be a subring of $\mathbb{Z}[x]$. Furthermore, if $p(x)$ is in this set and $q(x)$ is any element of $\mathbb{Z}[x]$, then $p(x)q(x)$ and $q(x)p(x)$ also have constant terms divisible by 3 since $p(x)$ does. Thus, the set is a subring closed under left and right multiplication by elements of $\mathbb{Z}[x]$ and thus must be an ideal.

(b) This isn't even a subring of $\mathbb{Z}[x]$. For example, x is in this set, since 0 is a multiple of 3, but $x \cdot x = x^2$ and 1 isn't a multiple of 3.

(c) This is closed under subtraction since subtraction is carried out component-wise. The set is also closed under multiplication since the power of x can't decrease through multiplication. Since the set is nonempty, it is a subring of $\mathbb{Z}[x]$. If $p(x)$ is in this set and $q(x) \in \mathbb{Z}[x]$, then consider the lowest degree term in $p(x)q(x)$. This will arise from the lowest degree terms in each of $p(x)$ and $q(x)$ and since the lowest possible degree for a term in $p(x)$ is 3, the lowest possible term in $p(x)q(x)$ is x^3. The argument for right multiplication follows similarly and so this set is an ideal.

(d) This set is not closed under multiplication by elements from $\mathbb{Z}[x]$. For example, 1 is in the set, but $1 \cdot x$ isn't.

(e) This set is clearly closed under subtraction since subtracting two sets of integers which sum to 0 will still sum to 0. If $p(x) = \sum_{i=1}^{n} a_ix^i$ and $q(x) = \sum_{j=1}^{m} b_jx^j$ then

$$p(x)q(x) = \sum_{i=1}^{n} a_ix^i \sum_{j=1}^{m} b_jx^j = \sum_{i=1}^{n} a_i \sum_{j=1}^{m} b_jx^{i+j}.$$

So in an unreduced form, $p(x)q(x)$ contains only terms obtained by taking $q(x)$ and multiplying it by each coefficient of $p(x)$. Thus, after we carry out the rest of the multiplication and look at the coefficients of the product, we can get back to the sum $\sum_{i=1}^{n} a_i \left(\sum_{j=1}^{m} b_j\right)$ by using the distributive property. But we know each of these terms is 0 since $q(x)$ is in our set. Furthermore, 0 is in the set so it's nonempty, and is thus a subring of $\mathbb{Z}[x]$. But now, in the preceding argument if we let $p(x)$ be an arbitrary element of $\mathbb{Z}[x]$, the same argument holds and so we have closure under left multiplication. A similar argument holds for right multiplication and so this set is an ideal.

(f) This is not closed under multiplication by elements from $\mathbb{Z}[x]$. For example, x^2+1 has derivative $2x$ which evaluates to 0 at 0. But $x(x^2+1) = x^3+x$ which has derivative $3x^2+1$. This evaluates to 1 at 0. □

Problem 11 (7.3.15)**.** *Let X be a nonempty set and let $\mathcal{P}(X)$ be the Boolean ring of all subsets of X defined in Exercise 21 of Section 1. Let R be the ring of all functions from X into $\mathbb{Z}/2\mathbb{Z}$. For each $A \in \mathcal{P}(X)$ define the function $\chi_A : X \to \mathbb{Z}/2\mathbb{Z}$ by $\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$ (χ_A is called the* characteristic function of A *with values in $\mathbb{Z}/2\mathbb{Z}$). Prove that the map $\mathcal{P}(X) \to R$ defined by $A \mapsto \chi_A$ is a ring isomorphism.*

Proof. Let $A, B \in \mathcal{P}(X)$. Let $\varphi : \mathcal{X} \to R$ be defined as above. Note that

$$\chi_A(x) + \chi_B(x) = \begin{cases} 1 & \text{if } x \in A \text{ and } x \notin B \text{ or if } x \notin A \text{ and } x \in B \\ 0 & \text{if } x \in A \cap B \text{ or } x \notin A \text{ and } x \notin B. \end{cases}$$

and

$$\chi_A(x)\chi_B(x) = \begin{cases} 1 & \text{if } x \in A \cap B \\ 0 & \text{if } x \notin A \text{ or } x \notin B. \end{cases}$$

Now we have $\varphi(A+B) = \chi_{(A\setminus B)\cup(B\setminus A)}$. But this function is 1 when $x \in A$ and $x \notin B$ or when $x \in B$ and $x \notin A$ and 0 otherwise. By the first above statement we now have $\varphi(A+B) = \chi_A + \chi_B = \varphi(A) + \varphi(B)$. Next, by the second statement $\varphi(A \times B) = \chi_{A\cap B} = \chi_A\chi_B = \varphi(A)\varphi(B)$. Thus, φ respects the operations in each ring. Suppose now that $A \neq B$. Then there exists $x \in A$ such that $x \notin B$. But then $\varphi(A)(x) = \chi_A(x) = 1 \neq \chi_B(x) = \varphi(B)$. Thus, φ is injective. Finally, let $\psi \in R$ and let $C \subseteq X$ be the subset such that $x \in C$ if $\psi(x) = 1$ and $x \notin C$ if $\psi(x) = 0$. It's clear then that $\varphi(C) = \chi_C = \psi$ and so φ is injective. This concludes the proof that φ is a bijective homomorphism from $\mathcal{P}(X)$ to R. □

Problem 12 (7.3.24)**.** *Let $\varphi : R \to S$ be a ring homomorphism.*
(a) Prove that if J is an ideal of S then $\varphi^{-1}(J)$ is an ideal of R. Apply this to the special case when R is a subring of S and φ is the inclusion homomorphism to deduce that if J is an ideal of S then $J \cap R$ is an ideal of R.
(b) Prove that if φ is surjective and I is an ideal of R then $\varphi(I)$ is an ideal of S give an example where this fails if φ is not surjective.

Proof. (a) Let $a, b \in \varphi^{-1}(J)$. Then $\varphi(a), \varphi(b) \in J$, so $\varphi(a) - \varphi(b) = \varphi(a-b)$ is in J. Thus $a - b \in \varphi^{-1}(J)$. Likewise, $\varphi(a)\varphi(b) = \varphi(ab)$ is in J so $ab \in \varphi^{-1}(J)$. Since $1 \in J$, $\varphi^{-1}(1)$ is nonempty. This shows that $\varphi^{-1}(J)$ is a subring of R. Now let $r \in R$ and $a \in \varphi^{-1}(J)$. Then $\varphi(ra) = \varphi(r)\varphi(a)$. This is an element of J since J is an ideal of S. Thus $ra \in \varphi^{-1}(J)$ and so $\varphi^{-1}(J)$ is closed under left multiplication by elements of R. A similar argument shows that it is closed under right multiplication and these together show that it must be an ideal.

In the special case that φ is the inclusion homomorphism from R a subring of S, then $\varphi^{-1}(J)$ is a subset of both R and S and only includes elements of J. In particular, $\varphi^{-1}(J) = J \cap R$. By the above argument, this shows that $J \cap R$ is a an ideal of R.

(b) Suppose φ is surjective and I is an ideal of R. Let $a, b \in \varphi(I)$. Then there exists $c, d \in R$ such that $\varphi(c) = a$ and $\varphi(d) = b$. Since I is an ideal of R we have $c - d \in I$ and $\varphi(c-d) = \varphi(c) - \varphi(d) = a - b$ is

in $\varphi(I)$. Likewise, $cd \in I$ so $\varphi(cd) = \varphi(c)\varphi(d) = ab$ is in $\varphi(I)$. Noting that $1 \in I$ so $\varphi(1) \in \varphi(I)$ and $\varphi(I)$ is nonempty shows $\varphi(I)$ is a subring of S. Now let $s \in S$. Since φ is surjective there exists $r \in R$ such that $\varphi(r) = s$. If $a \in \varphi(I)$ such that $\varphi(c) = a$, then $rc \in I$ since I is an ideal of R. Thus $\varphi(rc) = \varphi(r)\varphi(c) = sa$ is in $\varphi(I)$. Therefore $\varphi(I)$ is closed under left multiplication. A similar argument holds for right multiplication so $\varphi(I)$ is an ideal of S.

As a counterexample, suppose that R is a proper subring of S and φ is the identity homomorphism from R into S. If R is not an ideal of S then we have that R is an ideal in itself, but $\varphi(R) = R$ is not an ideal in S. More specifically, we can take part (d) from Problem 10 as an example. This is a subring of $\mathbb{Z}[x]$, but is not an ideal. Thus, the inclusion map from this set into $\mathbb{Z}[x]$ doesn't give an ideal as it's not surjective. □

Problem 13 (7.3.30)**.** *Prove that if R is a commutative ring and $\mathfrak{N}(R)$ is its nilradical then zero is the only nilpotent element of $R/\mathfrak{N}(R)$ i.e., prove that $\mathfrak{N}(R/\mathfrak{N}(R)) = 0$.*

Proof. Let $r + \mathfrak{N}(R) \in R/\mathfrak{N}(R)$. Suppose that $0 = \mathfrak{N}(R) = (r + \mathfrak{N}(R))^n = r^n + \mathfrak{N}(R)$. Thus, $r^n \in \mathfrak{N}(R)$. That is, $(r^n)^m = r^{nm} = 0$ for some positive integer m. But then r is a nilpotent element of R and so $r \in \mathfrak{N}(R)$ which means $r + \mathfrak{N}(R) = 0$. Therefore the only nilpotent element of $R/\mathfrak{N}(R)$ is 0. □

Problem 14 (7.3.36)**.** *Show that if I is the ideal of all polynomials in $\mathbb{Z}[x]$ with zero constant term then $I^n = \{a_n x^n + a_{n+1}x^{n+1} + \cdots + a_{n+m}x^{n+m} \mid a_i \in \mathbb{Z}, m \geq 0\}$ is the set of polynomials whose first nonzero term has degree at least n.*

Proof. Let $p(x) \in I^n$. Then $p(x)$ is a finite sum of m elements of the form $q_{1_1}(x)q_{1_2}(x)\ldots q_{1_n}(x)$ with $q_{i_j}(x) \in I$ for all i and j. The first nonzero term in $p(x)$ will be the sum over i of the product over j of all the first nonzero terms in each $q_{i_j}(x)$. If for all i some $q_{i_j}(x)$ is 0, then $p(x)$ is 0. Otherwise, note that the smallest possible nonzero term in each $q_{i_j}(x)$ is $b_{i_{j_1}}x$. Thus, the smallest possible first nonzero term in $p(x)$ is

$$\sum_{i=1}^{m}\prod_{j=1}^{n} b_{i_{j_1}}x = \sum_{i=1}^{m} x^n \prod_{j=1}^{n} b_{i_{j_1}} = a_n x^n$$

For some $a_n \in \mathbb{Z}$. Note that it's possible that $a_n = 0$ if the sum over i comes out to 0. It's also possible that $b_{i_{j_1}}$ is not the first nonzero term in $q_i(x)$. In these cases $b_{i_{j_k}}x^k$ with $k > 1$ will be the smallest term in $q_{i_j}(x)$ and this will only raise the exponent in the first nonzero term of $p(x)$. Thus, $I^n \subseteq \{a_n x^n + a_{n+1}x^{n+1} + \cdots + a_{n+m}x^{n+m} \mid a_i \in \mathbb{Z}, m \geq 0\}$.

Conversely, suppose $p(x) = a_n x^n + a_{n+1}x^{n+1} + \cdots + a_{n+m}x^{n+m}$ where $m \geq 0$ and $a_i \in \mathbb{Z}$. Then we can write $p(x)$ as

$$p(x) = a_n x \cdot x \ldots x + a_{n+1}x^2 \cdot x \ldots x + \cdots + a_{n+m}x^{m+1} \cdot x \ldots x$$

where each product has n terms. Since x and $a_i x^{i+1}$ are all in I, we see that $p(x)$ is a finite sum of products of n terms from I. Thus $p(x) \in I^n$ and we've shown both inclusions so the sets must be equal. □

Problem 15 (7.3.37)**.** *An ideal N is called* nilpotent *if N^n is the zero ideal for some $n \geq 1$. Prove that the ideal $p\mathbb{Z}/p^m\mathbb{Z}$ is a nilpotent ideal in the ring $\mathbb{Z}/p^m\mathbb{Z}$.*

Proof. Let $I = p^m\mathbb{Z}$ and $N = p\mathbb{Z}/p^m\mathbb{Z}$. Note that an element of N^m is a finite sum of products of elements from N. These products are of the form

$$(p_1^{a_1} + I)(p_2^{a_2} + I)\ldots(p_m^{a_m} + I) = p_1^{a_1}p_2^{a_2}\ldots p_m^{a_m} + I$$

for positive integers a_i. It's possible that a term in the product is 0, but then the entire product is 0, so we'll assume otherwise. Note that since $a_i \geq 1$ for each i, p^m is common to any of these products, and so it's common to every term in the finite sum. Thus, every element of N^m can be written as $p^m + I$ times a finite sum of products in the form above. But $p^m + I = 0$ in this ring, so $N^m = 0$. □

Problem 16. *What are the possible ring homomorphisms from $\mathbb{Z}[x]$ to $\mathbb{Z}$ ($\mathbb{Z}$ is the ring of integers)? What are their kernels?*

Proof. Let $f : \mathbb{Z}[x] \to \mathbb{Z}$ be a homomorphism. Note that the only homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$ are the identity and the trivial homomorphism. Clearly the trivial homomorphism is a homomorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}$, so assume f is nontrivial. Let $p(x) \in \mathbb{Z}[x]$ with $p(x) = a_n x^n + \cdots + a_0$. Then $f(p(x)) = f(a_n)f(x)^n + \cdots + f(a_0)$. Note that f restricted to constant terms is a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$ and since we've assumed f is nontrivial, we know $f(a_i) = a_i$ for all i. Therefore $f(p(x)) = a_n f(x)^n + \cdots + a_0$. Now note that $f(x) = n$ for some integer n, so $f(p(x)) = p(n)$. That is, f is just the evaluation homomorphism at some integer n. The kernel of f is the set of polynomials which get mapped to 0. That is, the set of polynomials which have a root at n. □

Problem 17. *Can there be a ring homomorphism from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}$ (keep in mind our convention for ring homomorphisms here!)?*

Proof. We can have the trivial homomorphism in which $\varphi(x) = 0$ for all $x \in \mathbb{Z}/p\mathbb{Z}$. Otherwise, we must have $\varphi(x) = 1 \neq 0 = \varphi(y)$ for some x and y and some φ. Suppose φ is such a homomorphism. Consider the element $p-1$ in $\mathbb{Z}/p\mathbb{Z}$ and note that $(p-1)^2 = p^2 + 2p + 1 = 1$. Thus $p-1 = (p-1)^{-1}$. The only elements of $\mathbb{Z}$ which have multiplicative inverses are 1, -1 and 0. We know $\varphi(1) = 1$ and $\varphi(0) = 0$ by necessity of homomorphisms. But then $0 = \varphi(0) = \varphi(1 + p - 1) = \varphi(1) + \varphi(p-1) = 1 + \varphi(p-1)$ and so $\varphi(p-1) = -1$. But now

$$-p = \varphi(p-1) + \cdots + \varphi(p-1) = \varphi((p-1) + \cdots + (p-1)) = \varphi(p(p-1)) = \varphi(p^2 - p) = \varphi(0) = 0$$

which is a contradiction. Thus, such a homomorphism cannot exist. □

Problem 18. *Use the quotient map of rings $k[x, y] \to k[x, y]/(xy-1)$ to show that a surjective map of rings doesn't necessarily induce a surjective map on their groups of units.*

Proof. In the ring $k[x, y]$ the only possible units are elements of the form $r + 0 \times x + 0 \times y$ for $r \in k$. The quotient map from $k[x, y]$ to $k[x, y]/(xy - 1)$ is clearly surjective, and it maps $r \in k[x, y]$ to $r + (xy - 1)$. But now note that $(x + (xy - 1))(y + (xy - 1)) = xy + (xy - 1) = 1 + (xy - 1)$. Therefore $x + (xy - 1)$ and $y + (xy - 1)$ are both units in the quotient ring despite the fact that they are not the image of a unit in $k[x, y]$. □