3 Properties of Ideals

When solving a particular problem Y, you may appeal to the result of any problem X that has occurred before Y (earlier problem sheets included) whether or not you submitted a solution of problem X.

1/25: **3.1.** How many maximal ideals does the ring $\mathbb{Z}/a\mathbb{Z}$ possess under the following conditions?

General treatment.
Lemma 1: Let I be a nonzero ideal of $\mathbb{Z}/a\mathbb{Z}$, and let $n = |I|$. Then $n \mid a$ and

$$I = \left\{0, \frac{a}{n}, \frac{2a}{n}, \dots, \frac{(n-1)a}{n}\right\}$$

Proof: Since I is an ideal of $\mathbb{Z}/a\mathbb{Z}$, $(I,+) \leq (\mathbb{Z}/a\mathbb{Z},+)$. Thus, by Lagrange's theorem, $n = |I|$ divides $a = |\mathbb{Z}/a\mathbb{Z}|$. As to the other part of the lemma, since I is nonzero, there exists $m \in I$ such that $0 < m < a$. Since I is closed under multiplication, it follows that $0m, 1m, 2m, \dots, (a-1)m \in I$ (all of these numbers must be taken modulo a). However, some of these numbers may well be the same: If we define n by $\text{lcm}(a,m) = nm$, then we can see that $nm \equiv 0m \bmod a$, $(n+1)m \equiv 1m \bmod a$, and so on. Thus,

$$I = \{0m \bmod a, 1m \bmod a, 2m \bmod a, \dots, (n-1)m \bmod a\}$$

It follows since $(n-1)m < a$ and $nm \equiv 0 \mod a$ that $nm = a$ and hence $m = a/n$. Substituting this definition of m into the above yields the desired result.

Definition: Suppose that the prime factorization of a is $p_1^{e_1} \cdots p_m^{e_m}$ for some distinct prime numbers $p_1, \dots, p_m$ and natural numbers $e_1, \dots, e_m$. Since $n \mid a$ by Lemma 1, $n = p_1^{d_1} \cdots p_m^{d_m}$ where $0 \leq d_i \leq e_i$ $(i = 1, \dots, m)$. Let $\boldsymbol{I(d_1, \dots, d_m)}$ denote the ideal of the form given by Lemma 1, where $n = p_1^{d_1} \cdots p_m^{d_m}$.

Lemma 2: If $c_i \leq d_i$ $(i = 1, \dots, m)$, then $I(c_1, \dots, c_m) \subset I(d_1, \dots, d_m)$. If any one of the inequalities is strict, the set inclusion is proper.

Proof: We have that

$$I(c_1, \dots, c_m) = \left\{\frac{ja}{p_1^{c_1} \cdots p_m^{c_m}}\right\}_{j=0}^{p_1^{c_1} \cdots p_m^{c_m} - 1} \qquad I(d_1, \dots, d_m) = \left\{\frac{ja}{p_1^{d_1} \cdots p_m^{d_m}}\right\}_{j=0}^{p_1^{d_1} \cdots p_m^{d_m} - 1}$$

Let $r = \frac{p_1^{d_1} \cdots p_m^{d_m}}{p_1^{c_1} \cdots p_m^{c_m}}$. Then

$$I(c_1, \dots, c_m) = \left\{\frac{jra}{p_1^{d_1} \cdots p_m^{d_m}}\right\}_{j=0}^{p_1^{c_1} \cdots p_m^{c_m} - 1} \subset \left\{\frac{ja}{p_1^{d_1} \cdots p_m^{d_m}}\right\}_{j=0}^{p_1^{d_1} \cdots p_m^{d_m} - 1} = I(d_1, \dots, d_m)$$

as desired. Any inequality being strict is equivalent to $r > 1$ and hence $I(d_1, \dots, d_m)$ contains an element (specifically, $ja/p_1^{d_1} \cdots p_m^{d_m}$) that $I(c_1, \dots, c_m)$ does not, for example.

Theorem: $\mathbb{Z}/a\mathbb{Z}$ has m maximal ideals.

Proof: Consider the m ideals $M_i = I(e_1, \dots, e_i - 1, \dots, e_m)$. It follows by Lemma 2 that $M_i \subsetneq I(e_1, \dots, e_m) = \mathbb{Z}/a\mathbb{Z}$ and that there are no "intermediate" ideals. In particular, suppose that $I(d_1, \dots, d_m)$ is an ideal that contains M_i properly. Then $e_j \leq d_j \leq e_j$ for all $j \neq i$ and $e_i - 1 \leq d_i \leq e_i$. Moreover, since at least one inequality must be strict and none of the $j \neq i$ ones can be, we must have $d_i = e_i$. Therefore, $I(d_1, \dots, d_m) = I(e_1, \dots, e_m) = \mathbb{Z}/a\mathbb{Z}$. Therefore, the M_i are maximal.

Furthermore, any other ideal either has $d_i < e_i - 1$ or some additional $d_j < e_j$, leading to an additional intermediate ideal and negating the possibility of it being maximal. □

(i) $a = 81$.

Answer. $81 = 3^4$, so $\boxed{\text{one}}$. □

(ii) $a = 44$.

Proof. $44 = 2^2 \cdot 11$, so $\boxed{\text{two}}$. □

(iii) $a = 42$.

Proof. $42 = 2 \cdot 3 \cdot 7$, so $\boxed{\text{three}}$. □

3.2. Given ring homomorphisms $f : R \to A$ and $g : R \to B$, check that $h(v) = (f(v), g(v))$ for all $v \in R$ gives a ring homomorphism $h : R \to A \times B$.

Proof. To prove that h is a ring homomorphism, it will suffice to show that h respects addition and multiplication, and that $h(1_R) = 1_{A\times B}$.

Let $a_1, a_2 \in R$ be arbitrary. Then

$$\begin{aligned} h(a_1 + a_2) &= (f(a_1 + a_2), g(a_1 + a_2)) \\ &= (f(a_1) + f(a_2), g(a_1) + g(a_2)) \\ &= (f(a_1), g(a_1)) + (f(a_2), g(a_2)) \\ &= h(a_1) + h(a_2) \end{aligned}$$

and

$$\begin{aligned} h(a_1 \times a_2) &= (f(a_1 \times a_2), g(a_1 \times a_2)) \\ &= (f(a_1) \times f(a_2), g(a_1) \times g(a_2)) \\ &= (f(a_1), g(a_1)) \times (f(a_2), g(a_2)) \\ &= h(a_1) \times h(a_2) \end{aligned}$$

Additionally,

$$\begin{aligned} h(1_R) &= (f(1_R), g(1_R)) \\ &= (1_A, 1_B) \\ &= 1_{A\times B} \end{aligned}$$

These three sets of equations give all of the desired results. □

3.3. In particular, let I_1, I_2 be ideals of a commutative ring R, and let $\pi_i : R \to R/I_i$ $(i = 1, 2)$ be canonical surjections. Consider the ring homomorphism $h : R \to (R/I_1)\times(R/I_2)$ given by $h(a) = (\pi_1(a), \pi_2(a))$ for all $a \in R$.

(i) Describe $\ker(h)$ in terms of I_1, I_2.

Proof. The kernel of h is the set of all $a \in R$ such that

$$(0, 0) = 0 = h(a) = (\pi_1(a), \pi_2(a))$$

i.e., such that $\pi_i(a) = 0$ $(i = 1, 2)$. We know that $0 + I_i = 0 = \pi_i(a) = a + I_i$ when $a \in I_i$. Thus, putting everything back together, $a \in \ker(h)$ implies that $a \in I_i$ $(i = 1, 2)$, i.e., $a \in I_1 \cap I_2$. Additionally, if $a \in I_1 \cap I_2$, then $\pi_1(a) = \pi_2(a) = 0$. Therefore,

$$\boxed{\ker(h) = I_1 \cap I_2}$$

□

(ii) Prove that $A \implies B \implies C \implies A$.

(A) h is a surjection.

(B) $(0, 1)$ is in the image of h.

(C) $I_1 + I_2 = R$.

Proof. We tackle the implications one at a time.

(A) $\implies$ (B): Suppose h is a surjection. Then $\operatorname{im} h = (R/I_1) \times (R/I_2)$. Therefore, since $(0, 1) \in (R/I_1) \times (R/I_2)$, $(0, 1) \in \operatorname{im} h$.

(B) $\implies$ (C): Suppose $(0, 1) \in \operatorname{im} h$. Then there exists $a \in R$ such that $h(a) = (0, 1)$. Thus, by the definition of h, $a \in 0 + I_1 = I_1$ and $a \in 1 + I_2$. It follows from this latter statement that there exists $x \in I_2$ such that $a = 1 + x$, or $a + (-x) = 1$. Ideals are closed under multiplication by elements of R, so since $-1 \in R$, $-x \in I_2$. This combined with the fact that $a \in I_1$ demonstrates that that $1 = a + (-x) \in I_1 + I_2$. Therefore, since ideals are closed under multiplication, $I_1 + I_2 = R$.

(C) $\implies$ (A): Suppose $I_1 + I_2 = R$. Let $(x + I_1, y + I_2) \in (R/I_1) \times (R/I_2)$ be arbitrary. To prove that h is a surjection, it will suffice to find an $a \in R$ such that $h(a) = (x + I_1, y + I_2)$. Since $x, y \in R$, we know that $x, y \in I_1 + I_2$ by hypothesis. Thus, we may write $x = a_1 + a_2$ and $y = b_1 + b_2$, where $a_1, b_1 \in I_1$ and $a_2, b_2 \in I_2$. It follows that

$$(x+I_1, y+I_2) = ((a_1+a_2)+I_1, (b_1+b_2)+I_2) = (a_2+I_1, b_1+I_2) = ((a_2+b_1)+I_1, (a_2+b_1)+I_2)$$

Therefore, choosing $a = a_2 + b_1$, we have

$$h(a) = (x + I_1, y + I_2)$$

as desired. □

(iii) Assume that $I_1+I_2 = R$. Prove that $I_1I_2 = I_1 \cap I_2$. Deduce that $\phi : R/(I_1I_2) \to (R/I_1)\times(R/I_2)$ is an isomorphism.

Proof. To prove that $I_1I_2 = I_1 \cap I_2$, we will use a bidirectional inclusion proof. Since ideals are closed under multiplication by external elements and addition of internal elements, $I_1I_2 \subset I_1$ and $I_1I_2 \subset I_2$. Therefore, $I_1I_2 \subset I_1 \cap I_2$, as desired. Now let $x \in I_1 \cap I_2$ be arbitrary. Then $x \in I_1$ and $x \in I_2$. Now since $I_1 + I_2 = R$, we may pick $a_1 \in I_1$ and $a_2 \in I_2$ such that $a_1 + a_2 = 1$. Multiplying through this equation by x yields $xa_1 + xa_2 = x$. Moreover, since $x \in I_2$ and $a_1 \in I_1$, $xa_1 \in I_1I_2$. Similarly, $xa_2 \in I_1I_2$. It follows since I_1I_2 is closed under addition that $x = xa_1 + xa_2 \in I_1I_2$, as desired.

Since $h : R \to (R/I_1) \times (R/I_2)$ is a ring homomorphism and, by part (i), $\ker(h) = I_1 \cap I_2$, the NIT implies that h has a unique factorization $h = i \circ \phi \circ \pi$ where $\phi : R/(I_1 \cap I_2) \to (R/I_1) \times (R/I_2)$ is an isomorphism of rings. But since $I_1 \cap I_2 = I_1I_2$ by the above, we have that $\phi : R/(I_1I_2) \to (R/I_1) \times (R/I_2)$ is an isomorphism of rings, as desired. □

3.4. Prove that a nonzero ideal $I \subset F[[X]]$, where F is a field, is the principal ideal generated by X^n for some $n \geq 0$. (This is a continuation of Exercise 7.2.3c of Dummit and Foote (2004), addressed in HW2 Q2.2.)

Proof. Let I be an arbitrary nonzero ideal in $F[[X]]$, let n be the lowest power present in any polynomial in I, and let $f \in I$ be a polynomial with a nonzero X^n term. Since $a_n \neq 0$, f/X^n is a polynomial with nonzero constant term a_n. Additionally, since a_n is a nonzero element of a field, a_n is a unit. It follows by Exercise 7.2.3c that f/X^n is a unit. Thus, there exists $u \in R$ such that $u \times (f/X^n) = 1$. Multiplying through this equation by X^n yields

$$uf = X^n$$

Since $f \in I$ and $u \in F[[X]]$, $uf \in I$, so $X^n = uf \in I$. Multiplying any polynomial in $F[[X]]$ by the monic polynomial X^n can only increase the exponent of every term, so, to reiterate, there are no polynomials in I having terms with exponents less than n. Moreover, it follows by the Euclidean algorithm that every polynomial h with all terms having powers greater than or equal to n can be expressed as the product of some $q \in F[[X]]$ and X^n. Therefore, $I = (X^n)$. □

3.5. Recall that $R[X, Y] := R[X][Y]$. Regard R as a subring of $R[X, Y]$. Let R be a commutative ring.

The **universal property of $\boldsymbol{R[X,Y]}$** states: Let A be commutative. Given a ring homomorphism $\alpha : R \to A$ and $x, y \in A$, prove that there is a unique ring homomorphism $\beta : R[X, Y] \to A$ that satisfies $\beta(c) = \alpha(c)$ for all $c \in R$, $\beta(X) = x$, and $\beta(Y) = y$.

Deduce this statement from the universal property of $R[X]$.

Proof. Consider the ring homomorphism $\alpha : R \to A$ and the element $x \in A$ provided by the assumptions of the universal property of $R[X, Y]$. By the universal property of $R[X]$, we may link these to a unique ring homomorphism $\tilde{\alpha} : R[X] \to A$ such that $\tilde{\alpha}(a) = \alpha(a)$ for all $a \in R$ and $\tilde{\alpha}(X) = x$. If we now switch perspectives and view $R[X]$ as our ring, $\tilde{\alpha}$ as our coordinate change function on that ring, and y (from the original givens) as our element of interest in A, we can apply the universal property of "$R[X]$"[1] again. This time, it links $\tilde{\alpha}$ and y to a unique ring homomorphism $\beta : R[X][Y] \to A$ such that $\beta(a) = \tilde{\alpha}(a)$ for all $a \in R[X]$ and $\beta(Y) = y$.

Now we show that this β is the β we've been looking for. First off, note that $R[X, Y] = R[X][Y]$, so β has the correct domain and range. Additionally, we already have $\beta(Y) = y$. To show that $\beta(c) = \alpha(c)$ for all $c \in R$, let $c \in R$ be arbitrary. Since $R \subset R[X]$, $c \in R[X]$. Thus, $\beta(c) = \tilde{\alpha}(c)$. Additionally, since $c \in R$, we have from our original definition of $\tilde{\alpha}$ that $\tilde{\alpha}(c) = \alpha(c)$. Therefore, by transitivity, $\beta(c) = \alpha(c)$, as desired. Lastly, we wish to show that $\beta(X) = x$. Since $X \in R[X]$, we know that $\beta(X) = \tilde{\alpha}(X)$. Recall from the original definition of $\tilde{\alpha}$ that $\tilde{\alpha}(X) = x$. Therefore, by transitivity, $\beta(X) = x$, as desired. □

3.6. (i) For any $a \in R$, we may define the ring homomorphism $\phi : R[X] \to R$ by $\phi(f(X)) = f(a)$. Prove that $\ker \phi$ is a principal ideal, and find a generator of this ideal.

Proof. To prove that $\ker \phi$ is a principal ideal and identify its generator in the process, it will suffice to show that $\ker \phi = (X - a)$.

Suppose first that $f \in \ker \phi$. It follows by the definition of the kernel that $f(a) = \phi(f) = 0$. Additionally, recall from class that there exists $q \in R[X]$ such that

$$f(X) - f(a) = q(X)(X - a)$$

But since $f(a) = 0$, we have that

$$f = f - 0 = q \cdot (X - a) \in R[X](X - a) = (X - a)$$

as desired.

Now suppose that $f \in (X - a)$. Then $f = q \cdot (X - a)$ for some $q \in R[X]$. It follows that

$$\phi(f) = f(a) = q(a) \cdot (a - a) = q(a) \cdot 0 = 0$$

so $f \in \ker \phi$, as desired. □

(ii) Let $g \in R[X]$. Define $\phi : R[X, Y] \to R[X]$ by $\phi(f(X, Y)) = f(X, g(X))$. Prove that $\ker \phi$ is a principal ideal, and find a generator of this ideal.

Proof. To prove that $\ker \phi$ is a principal ideal and identify its generator in the process, it will suffice to show that $\ker \phi = (Y - g(X))$.

[1] Perhaps it would be more accurate to say "the universal property of $R[X][Y]$" at this point!

Suppose first that $f \in \ker \phi$. It follows by the definition of the kernel that $f(X, g(X)) = \phi(f) = 0$. Additionally, if we regard f as a polynomial in Y, the Euclidean algorithm asserts that there exist $q, r \in R[X, Y]$ such that

$$f(X,Y) = q(X,Y)(Y - g(X)) + r(X,Y)$$

where $\deg(r) < 1 = \deg(Y - g(X))$. It follows from this last statement that $\deg(r) \in \{0, -\infty\}$, i.e., r is a constant. We may determine its value by evaluating the above at $(X, g(X))$, as follows.

$$\begin{aligned} f(X, g(X)) &= q(X, g(X))(g(X) - g(X)) + r \\ r &= f(X, g(X)) \end{aligned}$$

Therefore,

$$\begin{aligned} f(X,Y) &= f(X,Y) - 0 \\ &= f(X,Y) - f(X, g(X)) \\ &= q(X,Y)(Y - g(X)) \\ &\in R[X,Y](Y - g(X)) \\ &= (Y - g(X)) \end{aligned}$$

as desired.

Now suppose that $f \in (Y - g(X))$. Then $f = q \cdot (Y - g(X))$ for some $q \in R[X, Y]$. It follows that

$$\phi(f) = f(X, g(X)) = q(X, g(X)) \cdot (g(X) - g(X)) = q(X, g(X)) \cdot 0 = 0$$

so $f \in \ker \phi$, as desired. □

3.7. Let a, b be elements of R a commutative ring, and let a be a unit of R. Consider the ring homomorphism $\phi : R[X] \to R[X]$ given by $\phi(f) = f(aX + b)$. Prove that ϕ is an isomorphism. *Hint*: It's inverse can be written down explicitly.

Proof. Let $\alpha : R \to R[X]$ be defined by $\alpha(c) = c$ for all $c \in R$. Given this ring homomorphism $\alpha : R \to R[X]$ as well as $(X - b)/a \in R[X]$, Q3.5 asserts that there is a unique ring homomorphism $\psi : R[X] \to R[X]$ that satisfies $\psi(c) = \alpha(c) = c$ for all $c \in R$ and $\psi(X) = (X - b)/a$. Since $\psi : R[X] \to R[X]$ defined by

$$\psi(f) = f\left(\frac{X - b}{a}\right)$$

satisfies both of these properties, it is the unique ring homomorphism that Q3.5 proved existed.

We now prove that $\phi \circ \psi = \psi \circ \phi = \mathrm{id}$. Let $f \in R[X]$ be arbitrary. Then

$$\begin{aligned} (\phi \circ \psi)(f) &= \phi(\psi(f)) \\ &= \phi\left(f\left(\frac{X-b}{a}\right)\right) \\ &= f\left(\frac{(aX+b) - b}{a}\right) \\ &= f(X) \\ &= \mathrm{id}(f) \end{aligned} \qquad \begin{aligned} (\psi \circ \phi)(f) &= \psi(\phi(f)) \\ &= \psi(f(aX + b)) \\ &= f\left(a \cdot \frac{X-b}{a} + b\right) \\ &= f(X) \\ &= \mathrm{id}(f) \end{aligned}$$

Therefore, ϕ is an isomorphism, as desired. □

3.8. Let R be an integral domain. Prove that every isomorphism $\phi : R[X] \to R[X]$ that satisfies $\phi(c) = c$ for all $c \in R$ is of the type given in Q3.7.

Proof. See the answer to Q3.7. What I did there (and, I guess, what I would need to repeat here) is invoke the universal property of $R[X]$ under an appropriate auxiliary function ($\alpha = \mathrm{id}$). This would then guarantee me existence and uniqueness for a ϕ satisfying $\phi(c) = c$. Additionally, we must have a monomial argument because anything with degree other than 1 would alter the possible degrees we can access in the image, thereby making ϕ *not* an isomorphism. By making the monomial as general as possible, i.e., with the two degrees of freedom a, b in $ax + b$, we can be sure to capture *all* relevant isomorphisms. □

3.9. (i) Exercise 7.1.11 of Dummit and Foote (2004): Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$, then $x = \pm 1$.

Proof. We have that

$$\begin{aligned} 1 &= x^2 \\ 0 &= x^2 - 1 \\ &= (x+1)(x-1) \end{aligned}$$

Since R is an integral domain, it contains no zero divisors, so either $x + 1 = 0$ (and $x = -1$) or $x - 1 = 0$ (and $x = 1$); either way, $x = \pm 1$, as desired. □

(ii) Deduce that $\{a^2 \mid 0 \neq a \in \mathbb{F}_p\}$ has cardinality $(p-1)/2$. Here, p is an odd prime, and $\mathbb{F}_p$ is the field of cardinality p.

Proof. There are $p - 1$ nonzero elements in $\mathbb{F}_p$. Although we usually think of these elements as $1, \dots, p - 1$, we can divide this list in two and consider instead the congruent elements

$$-\frac{p-1}{2}, \dots, -1, 1, \dots, \frac{p-1}{2}$$

Note that it is the fact that $p \geq 3$ is an odd prime that allows us to divide $p - 1$ (necessarily an even number) by 2 and still obtain a (nonzero) integer. Continuing, we can rearrange the list in this way because $a \equiv b \bmod p$ implies $a^2 \equiv b^2 \bmod p$, so it will not affect our operation of choice. Additionally, the boon is that choosing negative elements makes it very easy to see that $a^2 = (-a)^2$ for each $a \in \{1, \dots, (p-1)/2\}$. Therefore, for the $p - 1$ elements in the above list, there are only $(p - 1)/2$ squares: One for each distinct absolute value of an entry in the above list, as desired. □

3.10. Prove that there are exactly four rings of cardinality p^2, where p is a prime ($p = 2$ is included). Identify which of them is a field, which is a product of two fields, and find a nonzero nilpotent in both of the remaining cases.

Hint: First show that there are only two possibilities for the characteristic of such a ring. If the characteristic is an odd prime p, show that there is some θ in the ring with the two properties: (i) $\theta^2 \in \mathbb{F}_p$ and (ii) $1, \theta$ form a basis for the given ring viewed as an $\mathbb{F}_p$ vector space. Now apply the previous problem.

Proof. Tricky??

Yes – by far the hardest question. Show that $X^2 - \theta^2$ is a maximal ideal in the polynomial ring. If f is irreducible, then (f) is maximal. Check that $X^2 - \theta^2$ is irreducible.

Like 5 problems in 1 problem. Takes a bunch of techniques. The case where the square is zero is not hard. Write down four distinct rings and then use this to prove that you can't get any other ones. Keep them all in the quotient form?? One is a product of two cyclic groups; that's a product of fields. You're allowed to multiply differently when they're rings, not groups. 2 groups, but 4 rings. □