Homework 4 (Due Feb 19, 2025)

Jack Hyatt

MATH 547 - Algebraic Structures II - Spring 2025

June 8, 2025

Justify all of your answers completely.

1. Let R be a commutative ring and let I, J be ideals of R. Prove that each of the following subsets of R is also an ideal.

   (a) $I \cap J = \{x \in R : x \in I \text{ and } x \in J\}$

   Proof. First to show $I \cap J$ is a group with respect to $+$.
   Operation is associative. Since both I and J are ideals, they both contain additive inverses, the identity element, and are closed, so then their intersection is also all of that.
   Now to show the ideal part. Let $x \in I \cap J$ and $r \in R$. Then $x \in I$ and $x \in J$. Since they are ideals, then $rx \in I$ and $rx \in J$, meaning $rx \in I \cap J$. ∎

   (b) $I + J = \{x + y : x \in I, y \in J\}$

   Proof. First to show $I + J$ is a group with respect to $+$.
   The only non-trivial group property to show is inverses. Let $a = x + y \in I + J$. It is easy to see that $(-x) + (-y) \in I + J$ and is the inverse.
   Now to show the ideal part. Let $a = x + y \in I + J$ and $r \in R$. $ra = rx + ry$, and $rx \in I$ and $ry \in J$ since both are ideals. So $ra \in I + J$. ∎

   (c) $IJ = \{\sum_{k=1}^{n} a_k b_k : n \geq 0, a_k \in I, b_k \in J \ \forall k \in [n]\}$

   Proof. First to show IJ is a group with respect to $+$.
   Same operation as in R, so it is associative. The identity 0 is clearly in IJ. Inverses are also in IJ, take one inverse of a_k or b_k, just not both to get the inverse.
   Now for closure. Let $x, y \in IJ$ where $x = \sum_{k=1}^{n} a_k b_k$ and $y = \sum_{k=1}^{m} a'_k b'_k$. Then $x + y$ is just an even bigger sum, where each term is a product of an element from I and an element from J, meaning $x + y \in IJ$.
   Now to show the ideal part. Let $x \in IJ$ and $r \in R$, with $x = \sum_{k=1}^{n} a_k b_k$. $rx = \sum_{k=1}^{n} r a_k b_k$, and $r a_k \in I$ since I is an ideal. So $rx \in IJ$. ∎

2. Using the notation form problem 1:

   (a) Prove that if K is any ideal of R such that $I \subseteq K$ and $J \subseteq K$, then $I + J \subseteq K$ (i.e. $I + J$ is the smallest ideal fo R that contains both I and J).

   Proof. Assume the above assumption. Let $x + y \in I + J$. Then $x \in I$ and $y \in J$, meaning $x, y \in K$. Since K is an ideal, it is closed under addition, so $x+y \in K$. ∎

   (b) Prove that $IJ \subseteq I \cap J$.

   Proof. Let $x = \sum_{k=1}^{n} a_k b_k \in IJ$. Since I is an ideal, then any multiple of an element in I is also in I. So any $a_k b_k \in I$ since a_k is defined to be in I. Symmetric argument can be made for J. So every $a_k b_k \in I \cap J$. Since $I \cap J$ is an ideal, it is closed under addition, meaning $x \in I \cap J$. ∎

   (c) Give an example of two ideal I and J of the ring $\mathbb{Z}$ s.t. $I \neq J$ and $IJ \neq I \cap J$.

   Let $I = 4\mathbb{Z}$ and $J = 6\mathbb{Z}$. Clearly they are ideals and are not the same. It is not hard to see that $I \cap J = 12\mathbb{Z}$ (12 is the LCM of 4 & 6). It is also not hard to see that $IJ = 24\mathbb{Z}$, as every term is the sum will have a factor of 4 from I and a separate factor of 6 from J.

3. Let R be a commutative ring. Let I be the set of all the elements $x \in R$ with the property that $x^n = 0$ for some exponent $n \geq 0$ (the elements with this property are called nilpotent elements).

   (a) Prove that I is an ideal of R.

   Proof. First to show I is a group with respect to $+$.
   Same operation as in R, so it is associative. The identity 0 is clearly in I. For inverses, let $x \in I$ with $x^n = 0$. Take $-x \in R$. $(-x)^n = (-1)^n x^n = (-1^n)0 = 0$. So $-x \in I$.
   Now for closure. Let $x, y \in I$ where $x^n = 0$ and $y^m == 0$. Then $(x + y)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} x^i y^{n+m-i}$. When $i \leq n$, then $y^{n+m-i} = 0$ since the exponent is greater than m, and similarly for x^i when $i \geq n$. So every term is 0, meaning $(x+y)^{n+m} = 0$, showing $x + y \in I$.
   Now to show the ideal part. Let $x \in I$ and $r \in R$, with $x^n = 0$. $(rx)^n = r^n x^n = r^n 0 = 0$. So $rx \in I$. ∎

   (b) Let $R = \mathbb{Z}_n$, where $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ is the prime factorization of n. Prove that $[x]_n$ is a nilpotent element of R if and only if $p_1 \dots p_k$ divides x.

   Proof. $(\implies)$
   Assume $x^m \equiv 0$ for some $m \geq 0$. Then $x^m = nq$ for some integer q. So then $n \mid x^m$. So then n's prime factors must divide x.
   $(\impliedby)$
   Assume $p_1 \dots p_k \mid x$. Then $x = p_1 \dots p_k q$ for some integer q. Let $\alpha = \max\{\alpha_1, \dots, \alpha_k\}$. Then $x^\alpha = p_1^\alpha \dots p_k^\alpha q^\alpha$, which is a multiple of $p_1^{\alpha_1} \dots p_k^{\alpha_k} = n$. So then $x^\alpha \equiv 0 \mod n$, making $[x]_n$ a nilpotent element. ∎

4. Let $R = \mathbb{Z}[X]$. Let I denote the set of all the polynomials $f(X) \in \mathbb{Z}[X]$ that have an even number as the constant term.

   (a) Prove that I is an ideal of R.

   Proof. It is quite clear that I is a subgroup over addition, as 0 is even, even numbers have inverses, and are closed.

   Now to show the ideal part. Let $f(x) \in I$ and $r(x) \in R$. We care not for any terms of f or r except for the constant term. Denote f_0 and r_0 as the constants terms of f and r respectively, with the assumption that f_0 is even. Then the constant term of $f(x)r(x)$ is $f_0 r_0$, which is even since f_0 is even. So $f(x)r(x) \in I$. ∎

   (b) Find two polynomials $f_1(X), f_2(X)$ such that $I = (f_1(X), f_2(X))$.

   This is quite easy, as one of the functions needs to be 2 to take care of the constant being even, with the other needing to give access to different degrees, so x. So $I = (2, x)$.

   (c) Prove that I is not a principal ideal of R (cannot be generated by a single element; it follows that $\mathbb{Z}[X]$ is not a PID).

   Proof. BWOC, let $I = (f(x))$. Since f has to generate 2 and x, f must be a constant function that divides x. So then f is a unit in $\mathbb{Z}$. But the only units in $\mathbb{Z}$ are ± 1, which is not a polynomial with even constant. BOOM, A CONTRADICTION!!! ∎

   (d) Let J be the set of all polynomials in $\mathbb{Z}[X]$ that have an even number as the leading coefficient. Is J an ideal of R? Explain.

   No, as J is not closed under addition. Let $f = 2x^2 - x$ and $g = -2x^2$. We have $f + g = -x \notin J$.