E. Dummit's Math 4527 ~ Number Theory 2, Fall 2026 ~ Homework 5 Solutions

---

1. Determine, with brief reasons, whether each subset S is an ideal of the given ring R:

   (a) $R = F[x]$, $S =$ the set of polynomials whose coefficient of x is zero.

   - This subset is $\boxed{\text{not an ideal}}$ because it is not closed under arbitrary multiplication by elements of R: for example, $1 \in S$ but $x \cdot 1 = x$ is not in S.

   (b) $R = \mathbb{Z}/18\mathbb{Z}$, $S = \{0, 3, 6, 9, 12, 15\}$.

   - This set $\boxed{\text{is an ideal}}$ since $0 \in S$, S is closed under subtraction, and S is closed under arbitrary multiplication by elements of R since $x \cdot (3a) = 3(xa) \in S$.

   (c) $R = \mathbb{Z}/15\mathbb{Z}$, $S = \{0, 4, 8, 12\}$.

   - This set $\boxed{\text{is not an ideal}}$ since it is not closed under addition or multiplication (since neither $4+12 = 1$ nor $4 \cdot 4 = 1$ are in R).

   (d) $R = \mathbb{Z} \times \mathbb{Z}$, $S = \{(a, a) : a \in \mathbb{Z}\}$.

   - This set $\boxed{\text{is not an ideal}}$ because it is not closed under arbitrary multiplication by elements of R: for example, $(1, 1) \in S$ but $(1, 2) \cdot (1, 1) = (1, 2)$ is not in S.

   (e) $R = \mathbb{Z} \times \mathbb{Z}$, $S = \{(0, a) : a \in \mathbb{Z}\}$.

   - This set $\boxed{\text{is an ideal}}$ since it contains 0, is closed under subtraction, and is closed under arbitrary multiplication since $(x, y) \cdot (0, a) = (0, ay) \in S$.

   (f) $R = F[x]$, $S = F[x^2]$, the polynomials in which only even powers of x appear.

   - This set $\boxed{\text{is not an ideal}}$ as it is not closed under arbitrary multiplication: $x^2 \in S$ but $x \cdot x^2 = x^3 \notin S$.

   (g) $R = F[x]$, $S =$ the set of polynomials whose coefficients sum to zero.

   - This set $\boxed{\text{is an ideal}}$ since it is the kernel of the ring homomorphism $\varphi : F[x] \to F$ given by $\varphi(p) = p(1)$. (Of course, it is also possible to verify the ideal conditions explicitly.)

---

2. Let $R = \mathbb{Z}[\sqrt{7}]$ and consider the ideals $I = (3)$ and $J = (3, 1 + \sqrt{7})$.

   (a) Explain why R/I contains exactly 9 residue classes. [Hint: They are $p + q\sqrt{7} + I$ for $p, q \in \{0, 1, 2\}$.]

   - Note that I consists of the multiples of 3, so $I = \{3a + 3b\sqrt{7} : a, b \in \mathbb{Z}\}$. Thus, by subtracting an appropriate element from I, we see that any element of R is congruent to something of the form $p + q\sqrt{7}$ for $p, q \in \{0, 1, 2\}$.
   - On the other hand, all such elements are distinct modulo I, since none of their pairwise differences is in I. Therefore, the residue classes modulo I are uniquely represented by the 9 elements of the form $p + q\sqrt{7}$, and so the residue classes themselves have the form $p + q\sqrt{7} + I$ as claimed, and there clearly are $3 \cdot 3 = 9$ of them in total.

   (b) Write down the multiplication table for R/I, and identify which elements are units and which elements are zero divisors. Is I a prime ideal? A maximal ideal?

   - Here is the multiplication table (for brevity all entries are listed without the $+I$):

$\cdot$	0	1	2	$\sqrt{7}$	$1+\sqrt{7}$	$2+\sqrt{7}$	$2\sqrt{7}$	$1+2\sqrt{7}$	$2+2\sqrt{7}$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$\sqrt{7}$	$1+\sqrt{7}$	$2+\sqrt{7}$	$2\sqrt{7}$	$1+2\sqrt{7}$	$2+2\sqrt{7}$
2	0	2	1	$2\sqrt{7}$	$2+2\sqrt{7}$	$1+2\sqrt{7}$	$\sqrt{7}$	$2+\sqrt{7}$	$1+\sqrt{7}$
$\sqrt{7}$	0	$\sqrt{7}$	$2\sqrt{7}$	1	$1+\sqrt{7}$	$1+2\sqrt{7}$	2	$2+\sqrt{7}$	$2+2\sqrt{7}$
$1+\sqrt{7}$	0	$1+\sqrt{7}$	$2+2\sqrt{7}$	$1+\sqrt{7}$	$2+2\sqrt{7}$	0	$2+2\sqrt{7}$	0	$1+\sqrt{7}$
$2+\sqrt{7}$	0	$2+\sqrt{7}$	$1+2\sqrt{7}$	$1+2\sqrt{7}$	0	$2+\sqrt{7}$	$2+\sqrt{7}$	$1+2\sqrt{7}$	0
$2\sqrt{7}$	0	$2\sqrt{7}$	$\sqrt{7}$	2	$2+2\sqrt{7}$	$2+\sqrt{7}$	1	$1+2\sqrt{7}$	$1+\sqrt{7}$
$1+2\sqrt{7}$	0	$1+2\sqrt{7}$	$2+\sqrt{7}$	$2+\sqrt{7}$	0	$1+2\sqrt{7}$	$1+2\sqrt{7}$	$2+\sqrt{7}$	0
$2+2\sqrt{7}$	0	$2+2\sqrt{7}$	$1+\sqrt{7}$	$2+2\sqrt{7}$	$1+\sqrt{7}$	0	$1+\sqrt{7}$	0	$2+2\sqrt{7}$

- To compute these entries, we simply multiply and then reduce the coefficients of 1 and $\sqrt{7}$ modulo 3, so for example $(2\sqrt{7})(1+2\sqrt{7}) = 28 + 2\sqrt{7} \equiv 1 + 2\sqrt{7}$.
- The units are $\boxed{1, 2, \sqrt{7}, 2\sqrt{7}}$ and the zero divisors are $\boxed{1+\sqrt{7}, 2+\sqrt{7}, 1+2\sqrt{7}, 2+2\sqrt{7}}$.
- Since there are zero divisors in R/I, we see I is $\boxed{\text{not prime}}$ and hence also $\boxed{\text{not maximal}}$.

(c) Explain why R/J contains exactly 3 residue classes and identify them. Is J a prime ideal? A maximal ideal?

- Note that J contains I so the residue classes will be a subset of the ones we found above for R/I; we just have to decide which ones become equivalent when we include $1 + \sqrt{7}$.
- We can see that we end up with three inequivalent residue classes: $0 + J$, $1 + J$, and $2 + J$. Explicitly, we have $0 + J = \{(3a + b) + b\sqrt{7} : a, b \in \mathbb{Z}\}$, $1 + J = \{(3a + b + 1) + b\sqrt{7} : a, b \in \mathbb{Z}\}$, and $2 + J = \{(3a + b + 2) + b\sqrt{7} : a, b \in \mathbb{Z}\}$.
- From the description we gave here, we can see that the ring structure of R/J is isomorphic to $\mathbb{Z}/3\mathbb{Z}$, under the identification of $a + I$ with $\overline{a} \in \mathbb{Z}/3\mathbb{Z}$. The indices clearly add modulo 3, and we also have $(2 + J) \cdot (2 + J) = 4 + J = 1 + J$, so all of the multiplications also work consistently.
- Since $R/J \cong \mathbb{Z}/3\mathbb{Z}$ is isomorphic to a field, that tells us J is $\boxed{\text{maximal}}$, hence also $\boxed{\text{prime}}$.

---

3. Let R be a commutative ring with 1.

(a) If S is a not necessarily finite set of ideals of R, show that the intersection $T = \bigcap_{I \in S} I$ is an ideal of R.

- Let $x, y \in T$ and $r \in R$. Since $0 \in I$ for all $I \in S$ we see $0 \in T$; likewise, since $x - y$ and rx are also in I for all $I \in S$, they are also in the intersection T, so T is an ideal.

(b) Show via an explicit example that the union of a collection of ideals of R is not necessarily an ideal of R.

- There are many counterexamples. For example, $2\mathbb{Z} \cup 3\mathbb{Z} = \{\ldots, -3, -2, 0, 2, 3, 4, 6, \ldots\}$ is clearly not an ideal of $\mathbb{Z}$, since it contains 2 and 3 but not $3 - 2 = 1$.

(c) If $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ is a not necessarily finite increasing chain of ideals of R, show that the union $T = \bigcup_{i=1}^{\infty} I_i$ is an ideal of R.

- Let $T = \bigcup_i I_i$, let $x, y \in T$, and let $r \in R$. Then $0 \in T$ since $0 \in I_1$.
- By definition, we know that $x \in I_i$ and $y \in I_j$ for some i and j. Then for $a = \max(i, j)$, we see that x and y are both in I_a so since I_a is an ideal, we see that $x - y$ and rx are in I_a, hence in T as well.

---

4. Let R be a commutative ring with 1 and let I and J be ideals of R.

(a) Show that $I + J = \{a + b : a \in I, b \in J\}$, the set of all sums of elements of I and J, is an ideal of R.

- Clearly $0 \in I + J$, and if $r \in R$ and $x = a + b$ and $y = c + d$ are both in $I + J$, then so are $x - y = (a - c) + (b - d)$ and $rx = ra + rb$.

(b) Show that $I + J$ is the smallest ideal of R that contains both I and J. Deduce that if $I = (a_1, \ldots, a_n)$ and $J = (b_1, \ldots, b_m)$ then $I + J = (a_1, \ldots, a_n, b_1, \ldots, b_m)$.

- Certainly $I + J$ is an ideal that contains both I and J. Conversely, if an ideal contains both I and J then it also contains any element of the form $a + b$ for $a \in I$ and $b \in J$, hence contains $I + J$.
- Thus, $I + J$ is the smallest ideal that contains both I and J.
- If $I = (a_1, \ldots, a_n)$ and $J = (b_1, \ldots, b_m)$, then the ideal $(a_1, \ldots, a_n, b_1, \ldots, b_m)$ is the smallest ideal that contains both I and J, so it is also equal to $I + J$.

(c) Let a and b be positive integers with greatest common divisor d. Show that $(a) + (b) = (d)$ in $\mathbb{Z}$.

- By part (b) we have $(a) + (b) = (a, b) = (d)$, since we know that the ideal (a, b) is principal and generated by the gcd of a and b.

(d) Show that $IJ = \{a_1b_1 + \cdots + a_nb_n, : a_i \in I,\, b_i \in J\}$, the set of finite sums of products of an element of I with an element of J, is an ideal of R.

- Clearly $0 \in IJ$, and if $r \in R$ and $x = \sum a_ib_i$ and $y = \sum c_id_i$ are both in IJ, then so are $x - y = \sum a_ib_i + \sum(-c_i)d_i$ and $rx = \sum(ra_i)b_i$.

(e) If $I = (a_1, \ldots, a_n)$ and $J = (b_1, \ldots, b_m)$, show that $IJ = (a_1b_1, a_1b_2, \ldots, a_nb_1, a_1b_2, \ldots, a_nb_m)$.

- Clearly IJ contains all of the elements a_ib_j, so $(a_1b_1, a_1b_2, \ldots, a_nb_1, a_1b_2, \ldots, a_nb_m) \subseteq IJ$.
- Conversely, if $x = A_1B_1 + \cdots + A_nB_n \in IJ$, then we can write $A_i = r_{i,1}a_1 + \cdots + r_{i,n}a_n$ and $B_i = s_{i,1}b_1 + \cdots + s_{i,m}b_m$ for some elements $r_{i,j}, s_{i,j} \in R$.
- Then $A_iB_i = (r_{i,1}s_{i,1})a_1b_1 + \cdots + (r_{i,n}s_{i,m})a_nb_m$ is in IJ, hence so is x. Thus, $IJ = (a_1b_1, \ldots, a_nb_m)$.

(f) Show that IJ is an ideal contained in $I \cap J$, and give an example where $IJ \neq I \cap J$.

- If $x \in IJ$ then $x = a_1b_1 + \cdots + a_nb_n$ for some $a_i \in I$ and $b_i \in J$.
- Since each $a_i \in I$ and I is an ideal, we see that $a_1b_1, a_2b_2, \ldots, a_nb_n$ are each in I, hence so is their sum x.
- Likewise, since each $b_i \in J$ and J is an ideal, we see that $a_1b_1, a_2b_2, \ldots, a_nb_n$ are each in J, hence so is x. Thus, x is in both I and J, so $x \in I \cap J$. Thus, $IJ \subseteq I \cap J$.
- There are many examples where equality does not hold: a simple one is $I = J = 2\mathbb{Z}$ inside $\mathbb{Z}$: then $I \cap J = 2\mathbb{Z}$ while $IJ = 4\mathbb{Z}$, per part (e).

(g) If $I + J = R$, show that $IJ = I \cap J$. [Hint: There exist $x \in I$ and $y \in J$ with $x + y = 1$.]

- If $I + J = R$ then by definition there exist elements $x \in I$ and $y \in J$ with $x + y = 1$.
- Then for any $r \in I \cap J$, we can write $r = r(x + y) = rx + yr$, and both rx and yr are in IJ: hence $I \cap J \subseteq IJ$, and since $IJ \subseteq I \cap J$ by part (f), we conclude $IJ = I \cap J$.

---

5. Let R be a commutative ring with 1 and define the binomial coefficient $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ for integers $0 \leq k \leq n$. Prove the binomial theorem in R: $(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k$ for any $x, y \in R$ and any $n > 0$.

- First, we observe Pascal's identity $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ holds for every $0 \leq k \leq n$, either via $\binom{n-1}{k} + \binom{n-1}{k-1} = \frac{(n-1)!}{k!(n-k-1)!} + \frac{(n-1)!}{(k-1)!(n-k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$ or via a double-counting argument (if we choose k elements from a total of n, either we choose the last one or we do not).
- For the binomial theorem itself, we induct on n. The base case $n = 1$ is obvious, since $x + y = x + y$.
- For the inductive step, we have $(x + y)^n = (x + y)\sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-1-k}y^k = \sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-k}y^k + \sum_{j=0}^{n-1} \binom{n-1}{j} x^{n-1-j}y^{j+1} = \sum_{k=0}^{n-1} \left[\binom{n-1}{k} + \binom{n-1}{k-1}\right] x^{n-k}y^k = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k$, as desired.

---

6. Suppose R is a finite ring with $1 \neq 0$. If R has a prime number of elements p, show that R is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ as a ring. [Hint: Use Lagrange's theorem on the additive group of R to show 1 has additive order p, then consider the map $\varphi : \mathbb{Z} \to R$ with $\varphi(n) = n1_R$.]

- Per the hint, by Lagrange's theorem on the additive group of R, we see that the additive order of 1 must divide p. Since p is prime and the order cannot be 1 since $1 \neq 0$, the order must be p.
- Now consider the map $\varphi : \mathbb{Z} \to R$ given by $\varphi(n) = n1_R$.
- This map is a ring homomorphism since $\varphi(a + b) = (a + b)1_R = a1_R + b1_R = \varphi(a)\varphi(b)$ and $\varphi(ab) = (ab)1_R = (a1_R)(b1_R) = \varphi(a)\varphi(b)$, it is surjective because the p elements $\{n1_R : 0 \leq n \leq p - 1\}$ are distinct hence are all of the elements of R, and finally the kernel of φ is $p\mathbb{Z}$ since 1 has additive order p.
- Thus, by the first isomorphism theorem, $R \cong \mathbb{Z}/p\mathbb{Z}$.

---

7. Let F be a field and define $R = F[\epsilon]/(\epsilon^2)$, a ring known as ring of dual numbers over F. Intuitively, one can think of the element $\epsilon \in R$ as being like an "infinitesimal": a number so small that its square is zero.

   (a) Show that the zero divisors in R are the elements of the form $b\epsilon$ with $b \neq 0$, and the units in R are the elements of the form $a + b\epsilon$ with $a \neq 0$.

   - Notice that $(b\epsilon)(\epsilon) = 0$, so if $b \neq 0$ then $b\epsilon$ is a zero divisor.
   - Furthermore, if $a \neq 0$ then (motivated by the analogous calculation in $\mathbb{Q}(\sqrt{D})$) we can write $\frac{1}{a+b\epsilon} \cdot \frac{a-b\epsilon}{a-b\epsilon} = \frac{a-b\epsilon}{a^2}$. Thus, we see that $(a+b\epsilon)(a^{-1} - ba^{-2}\epsilon) = 1$, and so $a + b\epsilon$ is a unit.
   - Finally, since a zero divisor can never be a unit, and every nonzero element in R is of one of the above two forms, there are no other units or zero divisors.

   (b) Find the three ideals of R.

   - We claim that 0, R, and (ϵ) are the ideals of R. It is easy to see that they are all ideals.
   - Now suppose I is a nonzero proper ideal of R. Then I contains a nonzero element but cannot contain any units (since then we would have $I = R$): by part (a), the only possible remaining elements are therefore elements of the form $b\epsilon$ for some $b \neq 0$.
   - It is easy to see that $(b\epsilon) = (\epsilon)$ for any $b \neq 0$, so 0, R, and (ϵ) are the only ideals of R.

   (c) Let $p(x) \in F[x]$. Show that $p(x + \epsilon) = p(x) + \epsilon p'(x)$ in $R[x]$, where $p'(x)$ denotes the derivative of $p(x)$.

   - By the binomial theorem, we have $(x+\epsilon)^n = x^n + nx^{n-1}\epsilon + \binom{n}{2}x^{n-2}\epsilon^2 + \cdots + \epsilon^n$, but every term after the first two vanishes since each such term contains ϵ^2. Thus, $(x+\epsilon)^n = x^n + n\epsilon x^{n-1}$.
   - Then, for $p(x) = a_0 + a_1x + \cdots + a_nx^n$, we have $p(x+\epsilon) = a_0 + a_1(x+\epsilon) + \cdots + a_n(x+\epsilon)^n = a_0 + a_1(x+\epsilon) + a_2(x^2 + 2\epsilon x) + \cdots + a_n(x^n + n\epsilon x^{n-1}) = [a_0 + a_1x + \cdots + a_nx^n] + \epsilon(a_1 + 2a_2x + \cdots + na_nx^{n-1}) = p(x) + \epsilon p'(x)$.

   (d) Let $p(x), q(x) \in F[x]$ and set $P(x) = p(x)q(x)$. Show that $P'(x) = p'(x)q(x) + p(x)q'(x)$. [Hint: Use (c).]

   - On one hand, we have $P(x+\epsilon) = p(x+\epsilon)q(x+\epsilon) = (p(x) + \epsilon p'(x))(q(x) + \epsilon q'(x)) = p(x)q(x) + \epsilon[p'(x)q(x) + p(x)q'(x)]$ using (c) twice.
   - On the other hand, we have $P(x+\epsilon) = P(x) + \epsilon P'(x)$ again by (c). So comparing the expressions shows that we must have $P'(x) = p'(x)q(x) + p(x)q'(x)$, as claimed.

   Remark: Part (c) shows how to use dual numbers to give a purely algebraic way to compute the derivative of a polynomial (in fact, some computer systems actually do differentiation this way), and (d) illustrates that they yield a formal proof of the product rule. In fact, the dual numbers are essentially the same object used in the construction of cotangent spaces in differential geometry.

---

8. [Challenge] Let R be a commutative ring with 1. We say $x \in R$ is nilpotent if $x^n = 0$ for some integer $n \geq 1$.

   (a) If m is a positive integer, show that a is nilpotent in $\mathbb{Z}/m\mathbb{Z}$ if and only if every prime divisor of m also divides a.

   - Each such element is nilpotent in $\mathbb{Z}/m\mathbb{Z}$: if $m = p_1^{b_1} \cdots p_k^{b_k}$ and $a = r \cdot p_1p_2 \cdots p_k$, then $a^{\max(b_1,\ldots,b_k)}$ will be divisible by m, meaning that $a^{\max(b_1,\ldots,b_k)} \equiv 0 \pmod{m}$.
   - Conversely, suppose a is nilpotent in $\mathbb{Z}/m\mathbb{Z}$: this means that $a^n \equiv 0 \pmod{m}$ for some n, meaning that m divides a^n. Hence each prime divisor of m divides a^n.
   - By an easy induction using the fact that $p|xy$ implies $p|x$ or $p|y$, if p is prime and p divides a^n, then in fact p must divide a. Thus, a is divisible by each prime divisor of m, as required.

   (b) If x is nilpotent, show that $1 + x$ is a unit. Deduce that the sum of a unit and a nilpotent element is a unit. [Hint: Factor $1 + (-1)^n x^n$.]

   - For the first part, suppose that $x^n = 0$. Per the hint, we compute $(1+x)(1 - x + x^2 - x^3 + \cdots + (-1)^{n-1}x^{n-1}) = 1 + (-1)^n x^n = 1$, so $1 + x$ is a unit.
   - For the second part, if u is a unit and x is nilpotent, then xu^{-1} is also nilpotent, and $u + x = u(1 + xu^{-1})$. By the calculation above, $1 + xu^{-1}$ is a unit, as is u, hence so is their product $u + x$.

(c) Show that the set of nilpotent elements of R forms an ideal of R; this ideal is called the nilradical of R. [Hint: Use the binomial theorem to establish closure under subtraction.]

- Clearly 0 is nilpotent. Now suppose x and y are nilpotent, say with $x^n = y^m = 0$, and also let $r \in R$.
- From the binomial theorem (per problem 5), we see that every term in the expansion of $(x-y)^{m+n}$ contains either a factor of x^n or y^m, and is therefore zero. Also, $(rx)^n = r^n x^n = 0$ as well.
- Thus, the set of nilpotent elements contains 0, is closed under subtraction, and is closed under arbitrary R-multiplication, so it is an ideal.

(d) Show that the nilradical is contained in every prime ideal of R.

- If x is nilpotent, then $x^n = 0$ and thus $x^n \in P$ since any (prime) ideal contains 0.
- But now if P is prime if $x^n \in P$ then $x \cdot x^{n-1} \in P$ so $x \in P$ or $x^{n-1} \in P$; iterating (or applying a trivial induction on n) yields $x \in P$ in the second case also.

(e) Prove that the nilradical is the intersection of all the prime ideals of R. [Hint: If $a \in R$ is not nilpotent, let S be the set of all ideals not containing any power a^n, partially ordered by inclusion. Apply Zorn's lemma to show S has a maximal element I, and then show I is a prime ideal by noting that if $xy \in I$ but $x, y \notin I$ then $J = (x) + I$ and $K = (y) + I$ are not in S but have $JK \subseteq I$.]

- Following the hint, suppose $a \in R$ is not nilpotent and let S be the set of all ideals not containing any power a^n for $n \geq 0$. Then S contains the zero ideal (because a is not nilpotent, no power equals zero) so S is nonempty.
- Now suppose $\mathcal{C}$ is a chain in S: then the union $\cup_{I \in \mathcal{C}} I$ is an ideal (by the same argument used in the proof that maximal ideals exist) and it also does not contain any power a^n (by definition of union) hence it is in S and is thus an upper bound. In particular note that I is proper, since it does not contain a.
- By Zorn's lemma, S has a maximal element I. We claim I is prime: since it is proper, now suppose we had $x, y \in R$ such that $xy \in I$ but $x, y \notin I$.
- Following the hint again, letting $J = (x) + I$ we see J is an ideal properly containing I hence it is not in S (by maximality of I) so J contains some power a^n; in the same way $K = (y) + I$ contains some power a^m.
- But then $JK \subseteq (xy) + I = I$ but since $a^{m+n} \in JK$ this yields $a^{m+n} \in I$, which is impossible.
- Therefore, I is a prime ideal not containing a, so a is not contained in the intersection of all prime ideals. We conclude that any element in the intersection of all prime ideals must be nilpotent, so together with (d) this shows the nilradical is the intersection of all prime ideals.
