Math 566 - Homework 4
SOLUTIONS
Prof Arturo Magidin

1. Let R be a ring, and I an ideal of R. Show that if R is a principal ideal ring (a ring in which every ideal is principal), then R/I is a principal ideal ring. Do not assume R is commutative or has a unity.

   Proof. Let K be an ideal of R/I; we want to show that K is principal. By the Isomorphism Theorems, we know that K is an ideal of the form J/I, for some ideal J of R that contains I. Since we are assuming that R is a principal ideal ring, we know that there exists $a \in R$ such that $J = (a)$.

   We claim that $K = (a + I)$. Indeed, since $a \in J$, then $a + I \in \pi(J) = K$ (where $\pi\colon R \to R/I$ is the canonical projection); thus, K contains $(a + I)$, the smallest ideal of R/I that contains $a + I$. Thus, $(a + I) \subseteq K$.

   Now let $x \in K$. Then $x = \pi(b)$ for some $b \in J = (a)$. Thus, b can be written as

$$b = na + ra + as + \sum_{i=1}^{m} r_i a s_i,$$

   with $n \in \mathbb{Z}$, $m \in \mathbb{N}$, $r, s, r_i, s_i \in R$. Therefore,

$$\begin{aligned} x = \pi(b) = \pi\left(na + ra + as + \sum_{i=1}^{m} r_i a s_i\right) &= n\pi(a) + \pi(ra) + \pi(as) + \sum_{i=1}^{m} \pi(r_i a s_i) \\ &= n(a+I) + (r+I)(a+I) + (a+I)(s+I) + \sum_{i=1}^{m}(r_i + I)(a+I)(s_i+I). \end{aligned}$$

   Now we observe that each of $n(a+I)$, $(r+I)(a+I)$, $(a+I)(s+I)$, and $(r_i+I)(a+I)(s_i+I)$ lie in $(a+I)$, since it is an ideal; thus, $x \in (a+I)$, proving that $K \subseteq (a+I)$. Thus, K is principal generated by $a + I$, as desired. □

2. Let $R = \mathbb{Z}[\sqrt{-5}] = \left\{a + b\sqrt{-5} \;\middle|\; a, b \in \mathbb{Z}\right\}$. This is a unital subring of $\mathbb{C}$ (you may take this for granted). Define $N\colon R \to \mathbb{Z}$ by

$$N\left(a + b\sqrt{-5}\right) = \left(a + b\sqrt{-5}\right)\left(a - b\sqrt{-5}\right) = a^2 + 5b^2.$$

   (i) Show that N is multiplicative: if $x, y \in R$, then $N(xy) = N(x)N(y)$.

   Proof. We can note that $N(r) = r\overline{r}$ for each $r \in \mathbb{Z}[\sqrt{-5}]$, where $\overline{r}$ is the complex conjugate of r (since $R \subseteq \mathbb{C}$). Then the properties of complex conjugation give

$$N(rs) = (rs)(\overline{rs}) = r\overline{r}s\overline{s} = N(r)N(s).$$

   Or we can verify this directly: let $x = a + b\sqrt{-5}$, $y = r + t\sqrt{-5}$. Then:

$$\begin{aligned} N(xy) &= N\left((ar - 5bt) + (at + br)\sqrt{-5}\right) = (ar - 5bt)^2 + 5(at + br)^2 \\ &= a^2r^2 - 10abrt + 25b^2t^2 + 5a^2t^2 + 10abrt + 5b^2r^2 \\ &= a^2r^2 + 25b^2t^2 + 5a^2t^2 + 5b^2r^2. \\ N(x)N(y) &= (a^2 + 5b^2)(r^2 + 5t^2) = a^2r^2 + 5a^2t^2 + 5b^2r^2 + 25b^2t^2. \end{aligned}$$

   So we have equality. □

(ii) Show that $N(x) \geq 0$ for all $x \in R$, with equality if and only if $x = 0$.

Proof. Since $a, b \in \mathbb{Z}$, we have that $N(a + b\sqrt{-5}) = a^2 + 5b^2 \geq 0$, and $N(a + b\sqrt{-5}) = 0$ if and only if $a = b = 0$. □

(iii) Show that $N(x) = 1$ if and only if x is a unit in R. Determine all units of R.

Proof. If $N(x) = 1$, then $(a + b\sqrt{-5})(a - b\sqrt{-5}) = 1$, so $a + b\sqrt{-5}$ has $a - b\sqrt{-5}$ as a multiplicative inverse.

Conversely, if x is a unit, then there exists y such that $xy = 1$. Using (i), we have

$$1 = N(1) = N(xy) = N(x)N(y).$$

Since $N(x)$ and $N(y)$ are nonnegative integers, this implies that $N(x) = 1$.

So now suppose that $a + b\sqrt{-5}$ is a unit in R. Then $a^2 + 5b^2 = 1$, and since a, b are integers this forces $b = 0$. Thus, $a^2 = 1$, and hence the only units in R are 1 and -1. □

(iv) Show that if $a, b \in R$ and $a \mid b$ in R, then $N(a) \mid N(b)$ in $\mathbb{Z}$.

Proof. Suppose that $a, b \in R$ and $a \mid b$. Then there exists $x \in R$ such that $ax = b$, hence

$$N(b) = N(ax) = N(a)N(x).$$

Since $N(a)$, $N(x)$, and $N(b)$ are all integers, this shows that $N(a) \mid N(b)$ in $\mathbb{Z}$.

(v) Show that 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are irreducible in R.

Proof. Note that $N(2) = 4$, $N(3) = 9$, and $N(1 \pm \sqrt{-5}) = 6$. So none of them are units. They are certainly not zero.

If $2 = xy$ in R, then $N(x) \mid N(2) = 4$. If $N(x) = 1$, then x is a unit and we are done. Since $a^2 + 5b^2 = 2$ has no solutions with a and b integers, we cannot have $N(x) = 2$. And if $N(x) = 4$, then $N(y) = 1$, so y is a unit. Thus, if $2 = xy$, then either x is a unit or y is a unit, proving that 2 is irreducible.

Similarly, since $a^2 + 5b^2 = 3$ has no solutions with a and b integers, if $3 = xy$ holds in R, then $9 = N(x)N(y)$, so either $N(x) = 1$ (so x is a unit), or $N(x) = 9$ and then $N(y) = 1$ (so y is a unit). Thus, 3 is irreducible.

If $1 + \sqrt{-5} = xy$ and $N(x) \neq 1$, then it must equal 6 (since it cannot equal 2 or 3, but $N(1 + \sqrt{-5}) = 6$); so then $N(y) = 1$. Thus, either x or y are units, and hence $1 + \sqrt{-5}$ is irreducible. The exact same argument shows that $1 - \sqrt{-5}$ is also irreducible. □

(vi) Show that none of 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are prime.

Proof. Note that $(2)(3) = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

However, 2 cannot divide either $1 + \sqrt{-5}$ or $1 - \sqrt{-5}$, since $N(2) = 4$ does not divide $6 = N(1 \pm \sqrt{-5})$. Similarly, 3 cannot divide either, since $N(3) = 9$ does not divide 6. So both 2 and 3 divide a product but do not divide either factor, showing they are not prime.

Likewise, neither $1 + \sqrt{-5}$ nor $1 - \sqrt{-5}$ can divide 2 or 3, since $N(1 \pm \sqrt{-5}) = 6$ does not divide either $N(2) = 4$ nor $N(3) = 9$. So they both divide a product without dividing either factor, proving that they are not prime. □

3. A complex number z is an *algebraic integer* if and only if there is a monic polynomial $p(x)$ with integer coefficients,

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \qquad a_i \in \mathbb{Z}$$

such that $p(z) = 0$. The set $\mathbb{A}$ of all algebraic integers forms a subring of $\mathbb{C}$ (you may take this for granted).

(i) Prove that the only rational numbers that are algebraic integers are the integers.

Proof. Let a and b be integers, $b > 0$, $\gcd(a, b) = 1$, and assume that $\frac{a}{b}$ is an algebraic integer. Then there exists a monic polynomial with integer coefficients,

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

such that $p(\frac{a}{b}) = 0$. By the Rational Root Test, we know that $a \mid a_0$ and $b \mid 1$. Thus, $b = 1$, so $\frac{a}{b} = a \in \mathbb{Z}$. Hence, any rational number that is an algebraic integer must in fact be an integer.

Finally, if $a \in \mathbb{Z}$, then a is a root of $x - a$, so every integer is an algebraic integer. □

(ii) Prove that $\mathbb{A}$ is not a field, but has no irreducible elements and no primes.

Proof. To show that $\mathbb{A}$ is not a field, not that $2 \in \mathbb{A}$, but $\frac{1}{2} \notin \mathbb{A}$, by part (i). Thus, not every nonzero element of $\mathbb{A}$ has a multiplicative inverse, and thus $\mathbb{A}$ is not a field.

To show it has no irreducibles, we note that if α is an algebraic integer, and β is a complex number such that $\beta^2 = \alpha$, then β is an algebraic integer; that is, both complex square roots of an algebraic integer are algebraic integers.

Indeed, if α satisfies the polynomial

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with $a_i \in \mathbb{Z}$, and $\beta^2 = \alpha$, then β satisfies the polynomial

$$p(x^2) = x^{2n} + a_{n-1}x^{2(n-1)} + \cdots + a_1 x^2 + a_0,$$

which is a monic polynomial with integer coefficients. So β is an algebraic integer.

Now let $\alpha \in \mathbb{A}$ be a nonzero nonunit. If α is not a unit, and $\beta^2 = \alpha$, then β is not a unit: for if $\beta\gamma = 1$, then $\alpha\gamma^2 = 1$. And since such a β exists (because the complex numbers contain square roots of each complex number) it follows that α is not irreducible. Hence, $\mathbb{A}$ has no irreducibles.

Since prime elements are always irreducible in a domain, it follows that $\mathbb{A}$ has no prime elements either. □

4. A proper ideal I of a commutative ring with unity R is said to be a *primary ideal* if and only if for all $a, b \in R$, if $ab \in I$, then either $a \in I$ or $b^n \in I$ for some $n \geq 1$. Determine the primary ideals of $\mathbb{Z}$.

   Answer. Let (r) be an ideal of $\mathbb{Z}$, and suppose that (r) is primary. That means that if $r \mid ab$, then either $r \mid a$ or $r \mid b^n$ for some $n \geq 1$. This suggests that r must be the power of prime or 0.

   Indeed: let p be a prime, and consider (p^m), $m \geq 1$. If $p^m \mid ab$, let $k \geq 0$ be the largest integer such that $p^k \mid a$. If $k \geq m$, then $a \in (p^m)$. If $k < m$, then $p \mid b$, and therefore $p^m \mid b^m$, proving that $b^m \in (p^m)$. Thus, (p^m) is primary. And (0) is a prime ideal of $\mathbb{Z}$, and hence is primary.

   Conversely, if r is not a prime power and not 0. If r is a unit, then $(r) = \mathbb{Z}$ is not a proper ideal. If r is not zero, not a unit, and not a prime power, then there exist two primes, $p \neq q$, such that $p \mid r$ and $q \mid r$. Write $r = p^i q^j s$, where $i \geq 1$, $j \geq 1$, and s is an integer such that $p \nmid s$ and $q \nmid s$. Let $a = p^i$, $b = q^j s$. Then $a \notin (r)$ (since $q \mid r$ but $q \nmid a$); and $b^n \notin (r)$ for all $n \geq 1$ since $p \nmid b^n$. Thus, (r) is not a primary ideal. □

5. Let R be a commutative ring with unity, and let X be a nonempty subset of R. We say that d is a greatest common divisor of X if and only if

   (i) For every $x \in X$, $d \mid x$; and

   (ii) If $c \in R$ is such that $c \mid x$ for all $x \in X$, then $c \mid d$.

Prove that if R is a commutative principal ideal ring with unity, then every nonempty (possibly infinite) set of elements of R has a greatest common divisor.

Proof. Let X be a nonempty subset of R, and let (X) be the ideal generated by X. Since R is a principal ideal ring, then there exists $d \in R$ such that $(X) = (d) = Rd$ (the last equality because R is commutative with unity).

We prove that d is a greatest common divisor of X. If $x \in X$, then $x \in X \subseteq (X) = (d) = Rd$, so there exists $a \in R$ such that $x = ad$. Thus, $d \mid x$.

Now let $c \in R$ be such that $c \mid x$ for all $x \in X$. Then $x \in (c)$ for all $x \in X$, then $X \subseteq (c)$, and thus $(d) = (X) \subseteq (c)$. Since $(d) \subseteq (c)$, we have $c \mid d$, as required.

Thus, d is a greatest common divisor of X, as desired. $\square$

6. Let R be a commutative ring with unity. Show that if $x \in R$ is nilpotent, then $1_R - x$ and $1_R + x$ are both units.

   Proof. Let x be nilpotent, and let $n \geq 1$ be such that $x^n = 0$. If $n = 1$, then $x = 0$, so $1_R - x = 1_R$ is a unit. If $n > 1$, then

   $$(1_R - x)(1_R + x + x^2 + \cdots + x^{n-1}) = (1_R + x + x^2 + \cdots + x^{n-1}) - (x + x^2 + \cdots + x^n) = 1_R - x^n = 1_R,$$

   so $1_R - x$ is a unit. To finish, note that if x is nilpotent then so is $-x$, and therefore by what we have just shown it follows that $1_R - (-x) = 1_R + x$ is a unit. $\square$

7. Let R be a commutative ring, and let $A \subseteq R$. Let

   $$\sqrt{A} = \{r \in R \mid \text{there exists } n > 0 \text{ such that } r^n \in A\}.$$

   Prove that if I is an ideal of R, then $\sqrt{I}$ is an ideal of R that contains I. The ideal $\sqrt{I}$ is called the *radical of* I.

   Proof. Note that $\sqrt{I}$ is nonempty, since $I \subseteq \sqrt{I}$.

   Let $a, b \in \sqrt{I}$. Then there exists $n, m > 0$ such that $a^n \in I$ and $b^m \in I$. Then

   $$(a-b)^{n+m} = a^{n+m} + (-1)^{n+m} b^{n+m} + \sum_{j=1}^{n+m-1} \binom{n+m}{j} a^j b^{n+m-j}.$$

   Since $n, m > 0$ and I is an ideal, then $a^{n+m} = a^n a^m \in I$, and $b^{n+m} = b^n b^m \in I$. If $j \leq n$, then $n + m - j \geq m$, so $b^{n+m-j} \in I$, and if $j > n$ then $a^j \in I$. Hence, every summand in the expression lies in I.

   Thus, $(a-b)^{n+m} \in I$, which proves that $a - b \in \sqrt{I}$. Thus, $\sqrt{I}$ is a subgroup of R.

   Now let $a \in \sqrt{I}$ and $r \in R$. We need to show that $ra \in \sqrt{I}$. Since $a \in \sqrt{I}$, there exists $n > 0$ such that $a^n \in I$. Then $(ra)^n = r^n a^n \in I$ (since I is an ideal), so $ra \in \sqrt{I}$. This proves that $\sqrt{I}$ is an ideal. $\square$

8. Let R be a commutative ring with unity. Show that $\sqrt{(0)}$ is the ideal of all nilpotent elements of R (we proved the set of all nilpotent elements is an ideal in Homework 3) and that it is contained in every prime ideal of R.

   Proof. If a is nilpotent, then $a^n = 0$ for some $n \geq 1$, so by definition we have $a \in \sqrt{(0)}$. Conversely, if $a \in \sqrt{(0)}$, then there exists $n \geq 1$ such that $a^n \in (0) = \{0\}$, so a is nilpotent. Thus, $\sqrt{(0)}$ is the ideal of all nilpotent elements of R.

   To prove it is contained in every prime ideal of R, note that if P is a (completely) prime ideal in a (not necessarily commutative) ring R, and $a^n \in P$ for some $n \geq 1$, then $a \in P$. Indeed, inductively, if $n = 1$ then $a \in P$; and if $a^k \in P$ implies $a \in P$, and $a^{k+1} \in P$, then $aa^k \in P$, so either $a \in P$ or $a^k \in P$ and hence $a \in P$.

Now let a be a nilpotent element of R and P a prime ideal of R. Since R is commutative, P is completely prime. Since a is nilpotent, then $a^n = 0$ for some $n \geq 1$; thus, $a^n \in P$, hence $a \in P$. This shows every nilpotent element is contained in every prime ideal of R, so $\sqrt{(0)} \subseteq P$ for all prime ideals P. $\square$