Problem Set 10
solutions

Problem 1. Let R be a ring.

(1.1) Prove that an ideal I of R is proper if and only if I contains no units.

Proof. Let I be an ideal. If it contains no units, then it does not contain 1 and hence $I \neq R$. If I contains a unit u, then for all $r \in R$,

$$r = (ru^{-1})u \in I$$

and hence $I = R$. □

(1.2) Assume R is commutative. Show that R is a field if and only if its only ideals are $\{0\}$ and R.

Proof. Suppose R is a field. Every nonzero ideal I contains a nonzero element u, but since R is a field the element u must be unit. By (1.1), $I = R$. Assume R has exactly two ideals, $\{0\}$ and R. If $0 \neq a \in R$, then the ideal $(a) = Ra$ is nonzero, and thus $(a) = R$. In particular, there is $u \in R$ such that

$$au = ua = 1.$$

Thus a is a unit, and therefore R is a field. □

(1.3) Show that the only ideals of $R = \mathrm{Mat}_{2\times 2}(\mathbb{R})$ are $\{0\}$ and R, and yet R is not a division ring.

Proof. Let I be a nonzero ideal in R and suppose $A \in I$ is any nonzero matrix. By elementary linear algebra, we we may do row and column operations to get either

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \text{or} \qquad B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

Row and column operations amount to multiplying on the left or right by (invertible) matrices, so we can multiply A by other matrices on the left and/or right and obtain either I_2 or B. We conclude that $I_2 \in I$ or $B \in I$.

If $B \in I$, then we can apply a row operation and a column operation to B to obtain

$$C = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus $C \in I$. Therefore,

$$I_2 = B + C \in I.$$

Either way, we conclude that $I_2 \in I$, and thus $I = R$ by (1.1).

But R is not a division ring since it has many nonzero, nonunit elements; for example, B is nonzero but not invertible, since its determinant is zero and all invertible matrices have invertible determinant. □

Problem 2. Let a and b be nonzero integers. Prove that $(a, b) = (d)$ where $d = \gcd(a, b)$.

Proof. Since d divides a, then $a = dx$ for some integer x and $a \in (d)$. Similarly, $b \in (d)$. Hence $(a, b) \subseteq (d)$. By the Euclidean Algorithm (or a corollary of it), we can write $d = ax + by$ for some $x, y \in \mathbb{Z}$. Thus $d \in (a, b)$, so $(d) \subseteq (a, b)$. We conclude that $(a, b) = (d)$. □

Problem 3. Let I and J be ideals of a commutative ring R with $1 \neq 0$. In this problem, you can use without proof that $I+J$, $I \cap J$, and IJ are ideals of R.

(4.1) Show that $IJ \subseteq I \cap J$.

Proof. Recall that

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i \mid n \geqslant 0, a_i \in I, b_i \in J \right\}.$$

Given $a \in I$ and $b \in J$, since J is an ideal we have $ab \in J$, and since I is an ideal we have $ab \in I$. We conclude that $ab \in I \cap J$. Moreover, $I \cap J$ is an ideal and thus closed for sums, so for any $a_1, \ldots, a_n \in I$ and $b_1, \ldots, b_n \in J$ we must then have

$$\sum_{i=1}^{n} a_i b_i \in IJ.$$

Thus $IJ \subseteq I \cap J$ always holds. □

(4.2) Give an example where $IJ \neq I \cap J$.

Solution. Consider the ring $R = k[x]$, where k is any field, and let $I = J = (x)$. Then $I \cap J = I = (x)$, but $IJ = I^2 = (x^2) \neq I \cap J$.

(4.3) Suppose that $I + J = R$. Show that $IJ = I \cap J$.

Proof. If $I + J = R$, then there exist $i \in I$ and $j \in J$ such that $i + j = 1$. Let $\alpha \in I \cap J$, then $\alpha = \alpha \cdot 1 = \alpha \cdot (i + j) = ai + aj \in IJ$ and thus it follows that $I \cap J \subseteq IJ$ under the given hypotheses. □

(4.4) Suppose m and n are distinct maximal ideals of a commutative ring R. Prove that $mn = m \cap n$.

Hint: First consider $m + n$.

Proof. First note that $m + n$ is an ideal, and contains both m and n. Hence, $m + n$ properly contains both (as $m \neq n$), so we must have $m + n = R$. We conclude that $m \cap n = mn$. □

(4.5) Suppose that $I + J = R$. Show that there is a ring isomorphism $R/(I \cap J) \cong R/I \times R/J$.

Proof. Let $f\colon R \to R/I \times R/J$ be defined by

$$f(r) = (r + I, r + J).$$

This is a ring homomorphism:

- $f(r + s) = (r + s + I, r + s + J) = (r + I, r + J) + (s + I, s + J) = f(r) + f(s)$
- $f(rs) = (rs + I, rs + J) = (r + I, s + I)(r + J, s + J) = f(r)f(s)$.
- $f(1_R) = (1 + I, 1 + J) = 1_{R/I \times R/J}$.

Note that

$$\ker(f) = \{r \in R \mid r + I = 0 + I \text{ and } r + J = 0 + J\} = \{r \in R \mid r \in I \text{ and } r \in J\} = I \cap J.$$

Moreover, we claim that f is surjective. Since $I + J = R$, there exist $i \in I$ and $j \in J$ such that $i + j = 1$. Set $z := rj + si$. Now given any $(r + I, s + J)$, note that $si, ri \in I$ and $rj, sj \in J$, so

$$z + I = rj + si + I = rj + I = r(1 - i) + I = r - ri + I = r + I$$

and

$$z + J = rj + si + J = si + J = s(1 - j) + J = s - sj + J = s + J.$$

Thus

$$(r + I, s + J) = (z + I, z + J) = f(z).$$

By the UMP of quotient rings there is a well-defined ring homomorphism

$$\overline{f} : R/(I \cap J) \to R/I \times R/J$$

given by

$$\overline{f}(r + I \cap J) = (r + I, r + J).$$

Moreover, its kernel is $\{0\}$, since $\ker f = I \cap J$, and $\overline{f}$ is surjective since f is surjective. This shows $\overline{f}$ is an isomorphism. □

Problem 4. Define $N : \mathbb{C} \to \mathbb{R}$ to be the square of the complex norm; that is,

$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2.$$

You can use without proof that N satisfies $N(\alpha\beta) = N(\alpha)N(\beta)$ for any $\alpha, \beta \in \mathbb{C}$.

(2.1) Show that the only units of $\mathbb{Z}[i]$ are ± 1 and $\pm i$.

Proof. First, note that given $a + bi \in \mathbb{Z}[i]$, we have

$$N(a + bi) = a^2 + b^2 \in \mathbb{Z},$$

and in fact $N(a + bi) \geqslant 0$. If $\alpha\beta = 1$, then $N(\alpha)N(\beta) = 1$ and hence the nonnegative integers $N(\alpha)$ and $N(\beta)$ must satisfy $N(\alpha) = N(\beta) = 1$. We conclude that $\alpha \in \{\pm 1, \pm i\}$.

On the other hand, -1 is its own inverse and $i(-i) = 1$, so ± 1 and $\pm i$ are all units. □

(2.2) Prove that the only units of the ring $\mathbb{Z}[\sqrt{-5}]$ are ± 1.

Proof. Note that the norm of $\alpha = a + b\sqrt{-5}$ is $N(\alpha) = a^2 + 5b^2$. It α is a unit, then as in the previous proof its norm would have to be 1 and this can only occur if $a = \pm 1$ and $b = 0$. □

(2.3) Are there units in $\mathbb{Z}[\sqrt{2}]$ other than ± 1?

Solution: Yes, for instance $3 + 2\sqrt{2}$ is a unit since $(3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 9 - 4 \cdot 2 = 1$. Note that the trick we used on the Gaussian integers and $\mathbb{Z}[\sqrt{-5}]$ does not apply here, as the norm of $\alpha = a + b\sqrt{2}$ is

$$N(\alpha) = (a + b\sqrt{2})^2 = a^2 + ab\sqrt{2} + 2b^2.$$