

**Problem** (Problem 1): Let  $R$  be a Euclidean domain with norm  $N$ , and let

$$m = \min\{N(x) \mid x \in R \setminus \{0\}\}.$$

Show that any  $u \in R \setminus \{0\}$  satisfying  $N(u) = m$  is invertible.

**Solution:** Let  $u$  satisfy  $N(u) = m$ . Applying the division algorithm, we find that

$$1 = uq + r,$$

where  $r = 0$  or  $N(r) < N(u)$ . In the former case, we find that  $q = u^{-1}$ , while the latter case violates the assumption that  $N(u)$  is of minimal value.

**Problem** (Problem 2): Show that in a UFD every irreducible element is prime. Conclude that if  $R$  is a Noetherian domain, then  $R$  is a UFD if and only if every irreducible element is prime.

**Solution:** Let  $R$  be a UFD, and let  $h$  be an irreducible element such that  $h \mid ab$  for some  $a, b \in R$ .

Write the unique (up to associates) factorizations into irreducibles for  $a$  and  $b$ , giving

$$\begin{aligned} a &= a_1 a_2 \cdots a_r \\ b &= b_1 b_2 \cdots b_s. \end{aligned}$$

Therefore, for some  $k \in R$ , we have

$$hk = (a_1 a_2 \cdots a_r)(b_1 b_2 \cdots b_s).$$

Since  $h$  is irreducible, and the factorizations for  $a$  and  $b$  are unique up to associates, there is some  $u_j \in R^\times$  such that  $h = u_j a_j$  or some  $v_k \in R^\times$  such that  $h = v_k b_k$  (else we would have a different factorization for  $ab$  into irreducibles). Thus,  $h \mid a$  or  $h \mid b$  depending on which of these hold, so that  $h$  is prime.

Since we already know that primes are irreducible, it follows that, in a Noetherian domain, since every element has at least one factorization into irreducibles, such a factorization is unique if and only if every irreducible element is prime.

**Problem** (Problem 4): Let  $R$  be a domain in which every prime ideal is principal. Show that  $R$  is a PID by using the following suggestions.

- (i) Assume that the set of nonprincipal ideals is nonempty. Then, use Zorn's Lemma to find a maximal element  $I$  in it.
- (ii) Since  $I$  is not prime, there exist  $a, b \in R$  such that  $ab \in I$  but  $a, b \notin I$ . Let  $I_a = I + (a)$ , and let  $J$  be defined by

$$J = \{x \in R \mid xI_a \subseteq I\}.$$

Verify that  $J$  is an ideal of  $R$ . Deduce a contradiction by showing that  $I = I_a J$ .

**Solution:** Let  $\mathcal{X}$  be the set of all nonprincipal ideals of  $R$ , ordered by inclusion. Suppose toward contradiction that  $\mathcal{X}$  were nonempty. Let  $\{K_\alpha\}_{\alpha \in A} = \mathcal{C} \subseteq \mathcal{X}$  be a chain in  $\mathcal{X}$ , and let  $I = \bigcup_{\alpha \in A} K_\alpha$ , which is an upper bound for  $\mathcal{C}$ . We claim that  $I$  is nonprincipal.

Suppose not. Then,  $I = (v)$  for some  $v \in R$ ; since  $v \in I$ , it follows that  $v \in K_\alpha$  for some  $\alpha \in A$ , meaning that  $(v) \subseteq K_\alpha$ , or that  $K_\alpha = I = (v)$ , which would contradict the assumption that  $K_\alpha$  is nonprincipal.

Since  $I$  is nonprincipal,  $I$  is not prime, so there exists some  $ab \in I$  with  $a \notin I$  and  $b \notin I$ . Letting  $I_a = I + (a)$ , since  $I \subsetneq I_a$ , we must  $I_a = (u)$  for some  $u \in R$ .

Let

$$J = \{x \in R \mid x(I + (a)) \subseteq I\}.$$

Observe that  $J$  is closed under subtraction, since if  $x, y \in J$ , we have

$$\begin{aligned} (x - y)(I + (a)) &= x(I + (a)) - y(I + (a)) \\ &\subseteq I, \end{aligned}$$

since  $I$  is closed under subtraction. Similarly, if  $r \in R$ , then

$$\begin{aligned} rx(I + (a)) &= r(x(I + (a))) \\ &\subseteq I, \end{aligned}$$

since  $I$  is closed under multiplication by elements from  $R$ . Thus,  $J$  is an ideal. In particular, since  $J$  contains  $I$  and  $b \notin I$ ,  $J$  must be a principal ideal of the form  $(v)$ , so that  $I_a J = (uv)$  is principal as well.

Now, we observe that elements of  $I_a J$  are of the form

$$\begin{aligned} \sum_{k=1}^n (x_k + r_k a)(s_k v) &= \sum_{k=1}^n x_k(s_k v) + s_k v(r_k a) \\ &\in I, \end{aligned}$$

so that  $I_a J \subseteq I$ .

If  $x \in I$ , then since  $x \in I_a$ , and  $I_a = (u)$ , it follows that  $x = \ell u$  for some  $\ell \in R$ . Additionally, since  $rx \in I$  for arbitrary  $r \in R$ , it follows that  $r\ell u = \ell ru \in I$ , meaning that  $\ell(u) \subseteq I$ , meaning that  $\ell \in J$ . Thus,  $x \in I_a J$ , implying that  $I = I_a J$ , meaning  $I$  is principal, which is a contradiction of the fact that  $I$  is (allegedly) not principal.

**Problem** (Problem 5): Consider the following factorization into irreducibles in the ring  $R = \mathbb{Z}[\sqrt{-5}]$ :

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

9a Show that the elements  $2, 3, 1 \pm \sqrt{-5}$  are irreducible but not prime.

9b Next, consider the following 4 ideals:

$$P_1 = (2, 1 + \sqrt{-5})$$

$$P_2 = (2, 1 - \sqrt{-5})$$

$$P_3 = (3, 1 + \sqrt{-5})$$

$$P_4 = (3, 1 - \sqrt{-5}).$$

Show that all of  $P_1, P_2, P_3, P_4$  are prime ideals.

9c Show that  $P_1 P_3 = (1 + \sqrt{-5})$ ,  $P_2 P_4 = (1 - \sqrt{-5})$ ,  $P_3 P_4 = (3)$ , and  $P_1 = P_2$ .

**Solution:**

(a) We consider the norm  $N: \mathbb{Z}[\sqrt{-5}] \rightarrow \mathbb{N}$ , given by  $a + b\sqrt{-5} \mapsto a^2 + 5b^2$ . This norm is multiplicative, so we may establish the irreducibility of the elements  $2, 3, 1 \pm \sqrt{-5}$  using this norm. If there were a

factorization of 2 into non-units  $ab$ , then

$$\begin{aligned} 4 &= N(2) \\ &= N(a)N(b), \end{aligned}$$

implying that  $N(a) = N(b) = 2$  (as elements have norm 1 if and only if they are units). Yet, there are no  $x, y \in \mathbb{Z}$  such that  $x^2 + 5y^2 = 2$ , as we would have  $2 = x^2$  modulo 5, but the only squares in  $\mathbb{Z}/5\mathbb{Z}$  are 1 and 4.

Similarly, if there were a factorization of 3 into non-units  $ab$ , then

$$9 = N(a)N(b),$$

meaning that  $N(a) = N(b) = 3$ , so by a similar reasoning, if  $x^2 + 5y^2 = 3$ , then  $x^2 = 3$  modulo 5, which cannot happen by a similar reasoning.

Finally, if there were a factorization of  $1 \pm \sqrt{-5}$  into non-units  $ab$ , then

$$6 = N(a)N(b),$$

meaning  $N(a) = 2$  and  $N(b) = 3$  or vice versa. By similar reasoning, this cannot happen.

Additionally, observe that the units of  $\mathbb{Z}[\sqrt{-5}]$  are  $\pm 1$ , as  $x^2 + 5y^2 = 1$  for  $x, y \in \mathbb{Z}$  if and only if  $x = \pm 1$ .

Now, to see that  $2, 3, 1 \pm \sqrt{-5}$  are not prime, observe that  $2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ , but 2 does not divide either  $1 \pm \sqrt{-5}$ , as we have just established that they are irreducible, and similarly for 3 and vice versa.

(b) By the third isomorphism theorem, we see that

$$\mathbb{Z}[\sqrt{-5}]/P_1 \cong \frac{\mathbb{Z}[\sqrt{-5}]/(2)}{P_1/(2)}.$$

Focusing our attention on  $\mathbb{Z}[\sqrt{-5}]/(2)$ , we observe that an arbitrary  $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$  has the pair  $(a, b)$  satisfying either  $(0, 0)$ ,  $(0, 1)$ ,  $(1, 0)$ , or  $(1, 1)$  modulo 2, meaning that  $\mathbb{Z}[\sqrt{-5}]/(2)$  is an abelian group with four elements, none of which has order greater than 2, hence  $\mathbb{Z}[\sqrt{-5}]/(2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . Similarly, we see that  $P_1/(2)$  has elements of the form  $a + \alpha\sqrt{-5}$ , where  $\alpha \equiv 0$  or  $1$  modulo 2, hence  $P_1/(2)$  is isomorphic to  $\mathbb{Z}/2\mathbb{Z}$ . By the third isomorphism theorem, it then follows that  $\mathbb{Z}[\sqrt{-5}]/P_1 \cong \mathbb{Z}/2\mathbb{Z}$ , hence  $P_1$  is maximal (and thus prime).

Similarly, since

$$\mathbb{Z}[\sqrt{-5}]/P_2 \cong \frac{\mathbb{Z}[\sqrt{-5}]/(2)}{P_2/(2)},$$

we may use the same process as we showed for  $P_1$ , but with  $a - \alpha\sqrt{-5}$  instead of  $a + \alpha\sqrt{-5}$ , to show that  $\mathbb{Z}[\sqrt{-5}]/P_2 \cong \mathbb{Z}/2\mathbb{Z}$ .