

## Problem Set #2: More food for thought

In great attempts it is glorious even to fail.

**Instructions:** Do what must be done. Do not hesitate. Show no mercy. All assertions are to be read as challenges (“prove this!”).

### APPETIZERS

These problems are intended as numerical exercises and/or understanding checks.

0. Let  $R$  be a domain. For all  $a, b \in R$ , we have  $aR = bR \iff a = b(\text{unit})$ .

1. All of  $2, 3, 1 + \sqrt{-5}$ , and  $1 - \sqrt{-5}$  are irreducibles (atoms) of  $\mathbf{Z}[\sqrt{-5}]$ .

2. Finish the check from class that in the monoid  $\text{Id}(\mathbf{Z}[\sqrt{-5}])$ ,

$$\begin{aligned} (2) &= (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}), & (1 + \sqrt{-5}) &= (1 + \sqrt{-5}, 2)(1 + \sqrt{-5}, 3) \\ (3) &= (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}), & (1 - \sqrt{-5}) &= (1 - \sqrt{-5}, 2)(1 - \sqrt{-5}, 3). \end{aligned}$$

3. None of the ideals appearing on the RHS of the equations in Problem 2 are principal. That is, there is no  $\alpha \in \mathbf{Z}[\sqrt{-5}]$  with  $(2, 1 + \sqrt{-5}) = (\alpha)$ , and similarly for the other ideals there.

Hence, the monoid  $\text{Prin}(\mathbf{Z}[\sqrt{-5}])$  is properly contained in the monoid  $\text{Id}(\mathbf{Z}[\sqrt{-5}])$ .

4. In  $\text{Id}(\mathbf{Z}[\sqrt{-26}])$ , we have  $(3)(3)(3) = (1 + \sqrt{-26})(1 - \sqrt{-26})$ . “Explain” this as follows (in the sense of Leibniz’s Dream). Let

$$P = (3, 1 + \sqrt{-26}), \quad Q = (3, 1 - \sqrt{-26}).$$

Then

$$(3) = PQ, \quad (1 + \sqrt{-26}) = P^3, \quad (1 - \sqrt{-26}) = Q^3.$$

5. Let  $R = \mathbf{Z}[\sqrt{-3}]$  and let  $I = (2, 1 + \sqrt{-3})$ . Show that  $I^2 = 2I$  but that  $I \neq (2)$ . Why doesn’t this contradict the statement from class that all the monoids  $\text{Id}(\mathcal{O}_D)$  are UFM’s?

### MAIN COURSE

6. Suppose that  $M$  is a UFM (Unique Factorization Monoid). Establish Leibniz’s Dream: Whenever  $a, b, c, d \in M$  with  $ab = cd$ , there are  $r, s, t, u \in M$  with

$$a = rs, \quad b = tu, \quad c = rt, \quad d = su.$$

7. Let  $R$  be a Ring. Recall that if  $I, J$  are ideals of  $R$ , the product  $IJ$  is defined by

$$IJ = \{\text{all finite sums } a_1 b_1 + \cdots + a_m b_m : \text{each } a_i \in I, b_i \in J\}.$$

Check:

- a)  $IJ$  is an ideal of  $R$ .
- b) Ideal multiplication is commutative.
- c) Ideal multiplication is associative.
- d) The identity for multiplication is  $(1)$  (i.e.,  $R$  itself viewed as an ideal of  $R$ ).
- e)  $I(J + K) = IJ + IK$  for any three ideals  $I, J, K$ . Here the sum of two ideals is the set of all pairwise sums (which is indeed an ideal!).
- f)  $IJ \subseteq I \cap J$ .
- g) If  $I = \langle a_1, \dots, a_j \rangle$  and  $J = \langle b_1, \dots, b_k \rangle$ , then  $IJ = \langle a_1 b_1, \dots, a_1 b_k, \dots, a_j b_1, \dots, a_j b_k \rangle$ . (Here the generators are the pairwise products of the  $a$ 's and  $b$ 's.)
- h) If  $I, J$  are nonzero ideals and  $R$  is a domain, then  $IJ$  is nonzero.
- i) If  $IJ = (1)$ , then  $I = (1)$  and  $J = (1)$ .

8. Let  $D$  be a squarefree integer,  $D \neq 1$ . Put

$$\tau = \begin{cases} \sqrt{D} & \text{if } D \equiv 2, 3 \pmod{4}, \\ \frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \pmod{4}. \end{cases}$$

Recall that each element of  $\mathcal{O}_D$  has a unique expression in the form  $a + b\tau$  with  $a, b \in \mathbf{Z}$ .

Let  $I$  be a nonzero ideal of  $\mathcal{O}_D$  (where nonzero means that  $I \neq \{0\}$ ).

- a)  $I$  contains a positive integer.

Hint. Remember your friend named "NORM."

- b) Let  $n$  be the least positive element of  $I \cap \mathbf{Z}$ . Then  $I \cap \mathbf{Z} = n\mathbf{Z}$ .
- c)  $I$  contains an element  $a + b\tau$  with  $a, b \in \mathbf{Z}$  and  $b > 0$ . Let  $B$  be the least positive integer for which there exists an  $A \in \mathbf{Z}$  with  $A + B\tau \in I$ . Choose such an  $A$ . Then (in the ring  $\mathbf{Z}$ ) we have  $B \mid n$  and  $B \mid A$ .
- d)  $I = n\mathbf{Z} + (A + B\tau)\mathbf{Z}$ . Moreover, each element of  $I$  has a *unique* representation in the form  $nu + (A + B\tau)v$  for  $u, v \in \mathbf{Z}$ .
- e) Every element of  $\mathcal{O}_D$  is congruent, modulo  $I$ , to exactly one of  $u + v\tau$ , where  $0 \leq u < n$  and  $0 \leq v < B$ . Hence,  $\#\mathcal{O}_D/I = nB$ .

9. a) Let  $R$  be a domain and let  $K$  be the fraction field of  $R$ .<sup>1</sup> Suppose  $R$  is a UFD. Show that if  $\alpha \in K$  is a root of a monic polynomial  $x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$ , then  $\alpha \in R$ .

Imitate the proof of the Rational Root Test.

- b) Now let  $L$  be a quadratic field, say  $L = \mathbf{Q}[\sqrt{D}]$ , where  $D$  is squarefree. Show that if  $R$  is a subring of  $\mathcal{O}_D$  with

$$\mathbf{Z} \subsetneq R \subsetneq \mathcal{O}_D,$$

then  $R$  is *not* a UFD.

<sup>1</sup>Recall that "the fraction field" of  $R$  is any field  $K$  containing  $R$  (as a subring) all of whose elements have the form  $a/b$  with  $a, b \in R$  and  $b \neq 0$ . One such field can be constructed by mimicking the way one constructs  $\mathbf{Q}$  from  $\mathbf{Z}$ . All such fields are isomorphic, which licenses us to use the definite article.