MATH 702 – SPRING 2024
HOMEWORK 1
DUE MONDAY, JANUARY 29, 2020 BY THE BEGINNING OF CLASS.

1. **Prove that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.**

   Here is the plan.
   (a) Find all units in $\mathbb{Z}[\sqrt{-5}]$.
   (b) Observe that $3 \cdot 3 = 9 = (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5})$.
   (c) Observe that 3, $2 + \sqrt{-5}$, and $2 - \sqrt{-5}$ all are irreducible elements of $\mathbb{Z}[\sqrt{-5}]$, but $3 \neq u(2 + \sqrt{-5})$ for any unit u of $\mathbb{Z}[\sqrt{-5}]$.
   Let $|a + b\mathbb{i}| = \sqrt{a^2 + b^2}$ for $a, b \in \mathbb{R}$. Let $\theta = \sqrt{-5}$ and $R = \mathbb{Z}[\theta]$.

   (a) We first prove that ± 1 are the only units in R. Indeed, if $u = a + b\theta$ and v are units in R with $uv = 1$, then $|u|^2|v|^2 = u\bar{u}v\bar{v} = 1$; hence $(a^2 + 5b^2)|v|^2 = 1$ in $\mathbb{Z}$. The only units of $\mathbb{Z}$ are ± 1, thus, $(a^2 + 5b^2) = \pm 1$ so $b = 0$ and $a = \pm 1$. and
   (b) There is nothing for us to do.

   (c) It is clear that $3 \neq u(2 + \sqrt{-5})$ for any unit u (i.e., $u = \pm 1$) of $\mathbb{Z}[\sqrt{-5}]$. We show that 3, $2 + \theta$ and $2 - \theta$ are all irreducible in R. Suppose that any one of these numbers factors as

   $$\# = (a + b\theta)(c + d\theta)$$

   in R. Multiply by the conjugate equation to get

   $$9 = (a^2 + 5b^2)(c^2 + 5d^2)$$

   in $\mathbb{Z}$. The positive factors of 9 in $\mathbb{Z}$ are $1, 3, 9$. The factor $(a^2 + 5b^2)$ can not be 3. (If $b \neq 0$, then the factor is greater than 3. If $b = 0$, then 3 is not a perfect square in $\mathbb{Z}$.) So, $(a^2 + 5b^2)$ must be 1 or 9. So at least one of the factors $(a^2 + 5b^2)$ or $(c^2 + 5d^2)$ of 9 is 1. Thus, one of the factors $(a + b\theta)$ or $(c + d\theta)$ of # must be a unit in R.

2. **Express the ideal (2) in the ring $\mathbb{Z}[\sqrt{-5}]$ as the product of prime ideals. (If I and J are ideals of the (commutative) ring R, then IJ is the smallest ideal of R that contains all elements of the form ij with $i \in I$ and $j \in J$.)**

   I claim that $(2) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})$ and that each of the ideals $(2, 1 + \sqrt{-5})$ and $(2, 1 - \sqrt{-5})$ is a proper prime ideal of $R = \mathbb{Z}[\sqrt{-5}]$.

   It is clear that $(2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}) \subseteq (2)$. Indeed,

$$2(2) = 4 \in (2), \quad 2(1-\sqrt{-5}) \in (2), \quad 2(1+\sqrt{-5}) \in (2), \quad \text{and} \quad (1-\sqrt{-5})(1+\sqrt{-5}) = 6 \in (2).$$

   It is also clear that $(2) \subseteq (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})$. Indeed, we just calculated that 6 and 4 are in the ideal $(2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})$. It follows that $6 - 4$ is in $(2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})$.

If $(2, 1+\sqrt{-5})$ is a proper ideal R, then it is clear that $(2, 1+\sqrt{-5})$ is a maximal ideal of R (hence a prime ideal of R). Indeed, the only elements of $R/(2, 1+\sqrt{-5})$ are $\bar{0}$ and $\bar{1}$. (In particular, say, $\overline{\sqrt{-5}} = \overline{-1} = \bar{1}$.) It follows that there aren't any ideals of R with

$$(2, 1+\sqrt{-5}) \subsetneq \text{ideal} \subsetneq R.$$

A small calculation shows that $(2, 1+\sqrt{-5})$ is a proper ideal of R. Indeed, if $1 \in (2, 1+\sqrt{-5})$, then there are integers a, b, c, d with

$$1 = 2(a+b\sqrt{-5}) + (c+d\sqrt{-5})(1+\sqrt{-5}). \tag{0.0.1}$$

$$1 = 2a + c - 5d + \sqrt{-5}(2b+c+d).$$

Equate the real and imaginary parts of the preceeding equation to obtain the inequlaities:

$$1 = 2a + c - 5d \quad \text{and} \quad 0 = 2b + c + d.$$

Thus

$$1 = 2a + (c+d) - 6d \quad \text{and} \quad -2b = c + d.$$

Thus

$$1 = 2a - 2b - 6d.$$

The integer 1 is not an even integer; thus, the equation (0.0.1) has no solution and $(2, 1+\sqrt{-5})$ is a proper prime ideal of R.

One can repeat the argument to prove that $(2, 1-\sqrt{-5})$ is a proper prime ideal of R. Or a better idea is to prove that complex conjugation is an automorphism of R; then use the fact that an automorphism carries a prime ideal of R to a prime ideal of R.

This answer mainly came from Keith Conrad's notes:
`https://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf`

3. **Find a commutative domain R and an element r in R with r not 0, r not a unit, and r not equal to a finite product of irreducible elements of R.**

Consider the ascending chain of rings

$$\mathbb{Z}[x] \subseteq \mathbb{Z}[\sqrt[2]{x}] \subseteq \mathbb{Z}[\sqrt[4]{x}] \subseteq \mathbb{Z}[\sqrt[8]{x}] \subseteq \cdots .$$

Each of these rings is a polynomial ring in one variable over a PID; hence a UFD. Let

$$R = \bigcup_{n=1}^{\infty} \mathbb{Z}[\sqrt[2^n]{x}].$$

Observe that the only units of R are 1 and -1. Observe that if $f \in \mathbb{Z}[\sqrt[2^n]{x}]$, for some n, and f is irreducible in R, then f is also irreducible in $\mathbb{Z}[\sqrt[2^n]{x}]$. (The easiest way to see this is: any factorization in $\mathbb{Z}[\sqrt[2^n]{x}]$ remains a factorization in R and elements of $\mathbb{Z}[\sqrt[2^n]{x}]$ which are not units in $\mathbb{Z}[\sqrt[2^n]{x}]$ remain non-units in R.)

Observe that x is not zero in R, x is not a unit in R, and x can not be factored into a finite product of irreducible elements. Indeed, if x factored into a finite product of irreducible elements in R, then all of these irreducible factors would live in $\mathbb{Z}[\sqrt[2^n]{x}]$, for some n. The ring $\mathbb{Z}[\sqrt[2^n]{x}]$

is a UFD. The only factorization of x into irreducibles in $\mathbb{Z}[\sqrt[2^n]{x}]$ is $x = (\sqrt[2^n]{x})^{2^n}$. This is a contradiction because $\sqrt[2^n]{x}$ is not irreducible in R.

4. **Prove that $\mathbb{Z}[i]$ is a Euclidean domain. (Let R be a domain. Suppose that there is a function f from $R \setminus \{0\}$ to the set of non-negative integers with the property that whenever a and b are elements of R with b not zero, then there exists q and r in R such that $a = bq + r$ and either $r = 0$ or $f(r) < f(b)$. In this case R is called a <u>Euclidean Domain</u>.)**

Let $R = \mathbb{Z}[i]$. This answer mainly came from

`https://www.cmi.ac.in/~shreejit/Gaussian.pdf`

Let $f(\ell + mi) = \ell^2 + m^2$ for ℓ and m in $\mathbb{Z}$, not both zero. Observe that $f(r_1 r_2) = f(r_1)f(r_2)$ for r_1 and r_2 in $R \setminus \{0\}$.

First, we treat the case where $b \in \mathbb{Z}$ and $a = \ell + mi$, with ℓ and m in $\mathbb{Z}$ and $b \neq 0$. We find q_1, q_2, r_1, and r_2 in $\mathbb{Z}$ with $\ell = bq_1 + r_1$, $m = bq_2 + r_2$, and $-b/2 \leq r_1, r_2 \leq b/2$. Observe that

$$a = \ell + mi = b(q_1 + q_2 i) + (r_1 + r_2 i),$$

and either $r_1 + r_2 i = 0$ or

$$f(r_1 + r_2 i) = r_1^2 + r_2^2 \leq b^2/4 + b^2/4 < b^2 = f(b).$$

Now we treat the general case, $a, b \in R$ with $b \neq 0$. Apply the first case to the pair of elements $a\bar{b}$ and $b\bar{b}$ (where $\bar{\ }$ means complex conjugate). Of course, $b\bar{b}$ is positive integer. Find q and r in R with

$$a\bar{b} = qb\bar{b} + r \quad \text{and either } r = 0 \text{ or } \quad f(r) < f(b\bar{b}).$$

If $r = 0$, then $a\bar{b} = qb\bar{b}$ and $a = qb$ (because $b \neq 0$) and this is fine. Henceforth, assume $r \neq 0$. Observe that

$$(a - qb)\bar{b} = r$$

and

$$f(a - qb)f(\bar{b}) = f\big((a - qb)\bar{b}\big) = f(r) < f(b\bar{b}) = f(b)f(\bar{b}).$$

Thus,

$$f(a - qb) < f(b).$$

Hence,

$$a = qb + (a - qb) \quad \text{and} \quad f(a - qb) < f(b).$$

We have shown that R is a Euclidean domain.