MATH 4000/6000 – Homework #6

posted March 29, 2019; due by 5 PM on April 3, 2019

The beauty of mathematics only shows itself to [its] more patient followers. – Maryam Mirzakhani

Assignments are expected to be neat and stapled. **Illegible work may not be marked**. Starred problems (*) are required for those in MATH 6000 and extra credit for those in MATH 4000.

1. Exercise 3.3.2(b,c,e,h).

2. Let R be a commutative ring. Show that if $a_1, \dots, a_k$ are any elements of R, then the set $\langle a_1, \dots, a_k \rangle$ defined by

$$\langle a_1, \dots, a_k \rangle = \{r_1 a_1 + \cdots + r_k a_k : r_1, \dots, r_k \in R\}$$

is an ideal of R.

Remark: When $R = \mathbb{Z}$, the sets $\langle a, b \rangle$ for $a, b \in \mathbb{Z}$ showed up in your first homework assignment. There they were denoted $I(a, b)$.

3. Exercise 4.1.3. (In part (c), assume R is not the zero ring.)

4. Prove that every ideal of $F[x]$ is principal, i.e., of the form $\langle f(x) \rangle$ for some $f(x) \in F[x]$.

Hint: If 0 is the only element of the ideal, we can take $f(x) = 0$. Otherwise, take $f(x)$ as a nonzero element of the ideal whose degree is as small as possible. To conclude, apply the division algorithm.

5. Recall that $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$, and that for $z \in \mathbb{Z}[i]$, we defined $N(z) = z\bar{z}$. (Concretely, if $z = a + bi$, then $N(z) = a^2 + b^2$.)

In this exercise, we outline a proof of the following **division theorem for** $\mathbb{Z}[i]$:

Division theorem for $\mathbb{Z}[i]$**:** Let $a, b \in \mathbb{Z}[i]$, with $b \neq 0$. Then there exist $q, r \in \mathbb{Z}[i]$ with

$$a = bq + r, \quad \text{and} \quad N(r) < N(b). \tag{$\dagger$}$$

Example: Let $a = 10 + i$ and $b = 2 - i$. We have

$$10 + i = (2 - i)\overbrace{(4 + 2i)}^{q} + \overbrace{i}^{r},$$

where $1 = N(i) < N(2 - i) = 5$.

   (a) Explain (perhaps with a picture) why every complex number is within a distance $\frac{\sqrt{2}}{2}$ of some element of $\mathbb{Z}[i]$.

   Hint: Think about the complex plane. Where are the elements of $\mathbb{Z}[i]$ located there?

   (b) Given $a, b \in \mathbb{Z}[i]$ with $b \neq 0$, let $Q = a/b$. (Remember that $\mathbb{C}$ is a field, so a/b exists in $\mathbb{C}$.) From part (a), you can find a Gaussian integer q with $|a/b - q| \leq \frac{\sqrt{2}}{2}$. Prove that if we define $r := a - bq$, then ($\dagger$) holds. In fact, prove the stronger statement that $N(r) \leq \frac{1}{2}N(b)$.

   (c) Find q and r satisfying ($\dagger$) if $a = 5 + 7i$ and $b = 3 - i$.

6. Prove that every ideal of $\mathbb{Z}[i]$ is principal, i.e., of the form $\langle \alpha \rangle$ for some $\alpha \in \mathbb{Z}[i]$.

7. Exercise 4.1.14(c). Make sure to answer the two questions at the end (is it a field? is it an integral domain?).

8. Exercise 4.1.10. *Hint:* If you get stuck, try Exercise 4.1.9 first.

9. Let $a_1, \ldots, a_k \in \mathbb{Z}$. By Exercise 3, $\langle a_1, \ldots, a_k \rangle$ is an ideal of $\mathbb{Z}$. On the other hand, we proved in class that every ideal of $\mathbb{Z}$ has the form $\langle d \rangle$ for some integer d. Thus, there is a $d \in \mathbb{Z}$ with

$$\langle a_1, \ldots, a_k \rangle = \langle d \rangle.$$

Prove that d divides all the a_i, and that if e is any integer dividing all of the a_i then $e \mid d$. (In other words, d is a greatest common divisor of $a_1, \ldots, a_k$.)

10. (*) Let $R = \mathbb{Z}[x]$, and let I be the set of elements of R with even constant term. Show that I is an ideal of R but that I is not principal: there is no $f(x) \in \mathbb{Z}[x]$ with $I = \langle f(x) \rangle$.