MATH 4000/6000 – Homework #7

posted April 8, 2024; due April 17, 2024

> Many who have never had occasion to learn what mathematics is confuse it with arithmetic, and consider it a dry and arid science. In reality, however, it is the science which demands the utmost imagination.
> – Sofia Kovalevskaya[1]

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.

In this assignment "ring" always means "commutative ring."

1. Recall that the system of Gaussian integers was defined as $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$, 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 Algorithm for $\mathbb{Z}[i]$.

   Division Algorithm 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

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

   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? How is the distance between two elements related to the norm of their difference?

   (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 (†) holds. In fact, prove the stronger statement that $N(r) \leq \frac{1}{2}N(b)$.

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

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

3. Let R be a ring, and let I be an ideal of R. Prove that R/I is the zero ring if and only if $I = R$. (Remember that a ring is called "the zero ring" when its additive identity 0 is the same as its multiplicative identity 1.)

4. In class we stated that isomorphism functions as an equivalence on the class of rings. Here you are asked to show part of this, namely that isomorphism is symmetric.

   Suppose $\phi\colon R \to S$ is an isomorphism. Let $\psi\colon S \to R$ be the inverse function[2] of ϕ. Prove that ψ is an isomorphism. You may take as known that the inverse function of a bijection is a bijection.

5. (a) Let R be a ring, not the zero ring. We call an ideal $I \subseteq R$ a prime ideal if

   (i) $I \neq R$,

[1] Of note: `https://www.math.uga.edu/events/content/2024/sonia-kovalevsky-day-2024`

[2] 'Recall that 'inverse function" means $\psi(\phi(r)) = r$ for all $r \in R$ and $\phi(\psi(s)) = s$ for all $s \in S$.

(ii) whenever a and b are elements of R for which $ab \in I$, either $a \in I$ or $b \in I$ (or both).

Show that for every ideal I of R,

$$R/I \text{ is an integral domain} \iff I \text{ is a prime ideal of } R.$$

(b) What are all of the prime ideals of $\mathbb{Z}$? Justify your answer.

6. (a) By work in Chapter 3, every element of $\mathbb{Q}[\sqrt{2}]$ has a unique expression in the form $a+b\sqrt{2}$ where $a, b \in \mathbb{Q}$. Show that the map $\phi\colon \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$ defined by $\phi(a+b\sqrt{2}) = a-b\sqrt{2}$ is an automorphism of $\mathbb{Q}[\sqrt{2}]$.

   (b) Is the map $\phi\colon \mathbb{Q}[\sqrt{3}] \to \mathbb{Q}[\sqrt{7}]$ defined by $\phi(a+b\sqrt{3}) = a+b\sqrt{7}$ an isomorphism? Is there any isomorphism between $\mathbb{Q}[\sqrt{3}]$ and $\mathbb{Q}[\sqrt{7}]$?

7. Find the inverse of α^2+3 in $R = \mathbb{Z}_5[x]/\langle x^3-3x-2\rangle$. Here we use the notation from class, so that $\alpha = \overline{x}$ in R.

8. Let R be a ring.

   (a) If I and J are ideals of R, we let $I+J = \{i+j : i \in I, j \in J\}$. Show that $I+J$ is an ideal of R and that $I+J$ contains both I and J.

   (b) Let $a \in R$, and let I be an ideal of R. Suppose that $\langle a\rangle + I = R$, where $+$ is addition of ideals as defined in part (a). Show that $\overline{a}$ is a unit in R/I.

9. Use the Fundamental Homomorphism Theorem to establish the following ring isomorphisms.

   (a) $R/\langle 0\rangle \cong R$ for every ring R.

   (b) $\mathbb{R}[x]/\langle x^2+6\rangle \cong \mathbb{C}$.

   Hint: Consider the "evaluation at $i\sqrt{6}$" homomorphism taking $f(x) \in \mathbb{R}[x]$ to $f(i\sqrt{6}) \in \mathbb{C}$.

   (c) $\mathbb{Q}[x]/\langle x^2-1\rangle \cong \mathbb{Q}\times\mathbb{Q}$. *Hint:* Consider the homomorphism from $\mathbb{Q}[x]$ to $\mathbb{Q}\times\mathbb{Q}$ given by $f(x) \mapsto (f(1), f(-1))$.

10. (***; MATH 6000 problem**) Since $\mathbb{Z}[i]$ has a division algorithm, one can carry out versions of our previous arguments concerning Euclid's algorithm, gcds, the Fundamental gcd lemma, Euclid's lemma, and Unique Factorization.

    In particular, one can show the following version of Euclid's lemma in $\mathbb{Z}[i]$. Call π in $\mathbb{Z}[i]$ prime if π is not a unit in $\mathbb{Z}[i]$ but whenever we write $\pi = \alpha\beta$ with $\alpha, \beta \in \mathbb{Z}[i]$ either α is a unit or β is a unit.

    Euclid's lemma in $\mathbb{Z}[i]$: Suppose $\pi, \alpha, \beta \in \mathbb{Z}[i]$ with π prime. If $\pi \mid \alpha\beta$, then $\pi \mid \alpha$ or $\pi \mid \beta$.

    So far you are told all of this; you are not asked to prove any of the above.

    (a) Let p be an ordinary prime, meaning a prime in the integers (one of $2, 3, 5, 7, \dots$). Suppose there is an integer n for which $p \mid n^2+1$. Prove that p is *not* prime in $\mathbb{Z}[i]$.

    (b) (continuation) Continue with the assumptions of (a). Show that there are integers x, y with $p = x^2+y^2$.

11. (***; MATH 6000 problem**) Let p be a(n ordinary) prime with $p \equiv 1 \pmod 4$. Using your answer to HW #3 7(b), show that -1 is a square in $\mathbb{Z}_p$ for all these primes p. Deduce from the previous problem that $p = x^2+y^2$ for some integers x, y.

    By contrast, if p is a prime with $p \equiv 3 \pmod 4$, it is simple to show that p is not a sum of two squares (look at the squares mod 4). Hence, an odd prime p is a sum of two squares if and only if $p \equiv 1 \mod 4$. This result is sometimes called Fermat's Christmas Theorem as it appears in a letter of Fermat dated December 25.