Drexel University, Department of Mathematics

Math 332: Undergraduate Abstract Algebra II, Winter 2023: Midterm 2

Please solve **at most 3 of the 6 problems!** **No collaboration** is allowed on the midterm.

Darij Grinberg

March 10, 2023

1 Exercise 1

1.1 Problem

(a) Prove that there are no ring morphisms from $\mathbb{Z}[i]$ to $\mathbb{Z}$.

Now, let p be a prime number. Prove the following:

(b) There are no ring morphisms from $\mathbb{Z}[i]$ to $\mathbb{Z}/p$ if $p \equiv 3 \mod 4$.

(c) There are exactly two ring morphisms from $\mathbb{Z}[i]$ to $\mathbb{Z}/p$ if $p \equiv 1 \mod 4$.

(d) There is a unique ring morphism from $\mathbb{Z}[i]$ to $\mathbb{Z}/p$ if $p = 2$.

More generally, prove the following:

(e) If R is any ring, then the number of ring morphisms from $\mathbb{Z}[i]$ to R is the number of all elements $r \in R$ satisfying $r^2 = -1$.

1.2 Hint

If f is a ring morphism from $\mathbb{Z}[i]$ to R, then what equation must $f(i)$ satisfy?

1.3 Solution

...

---

2 Exercise 2

2.1 Problem

Let ω denote the complex number $\dfrac{-1+\sqrt{-3}}{2} \in \mathbb{C}$.

(a) Prove that $\omega^3 = 1$ and $\omega^2 + \omega + 1 = 0$.

(b) Prove that $|a + b\omega| = \sqrt{a^2 - ab + b^2}$ for any $a, b \in \mathbb{R}$.

(c) Define a subset $\mathbb{Z}[\omega]$ of $\mathbb{C}$ by

$$\mathbb{Z}[\omega] := \{a + b\omega \mid a, b \in \mathbb{Z}\}.$$

Prove that $\mathbb{Z}[\omega]$ is a subring of $\mathbb{C}$. (It is called the ring of *Eisenstein integers*.)

(d) Prove that $\mathbb{Z}\left[\sqrt{-3}\right]$ is a subring of $\mathbb{Z}[\omega]$.

(e) Prove that the ring $\mathbb{Z}[\omega]$ is Euclidean, and that the map

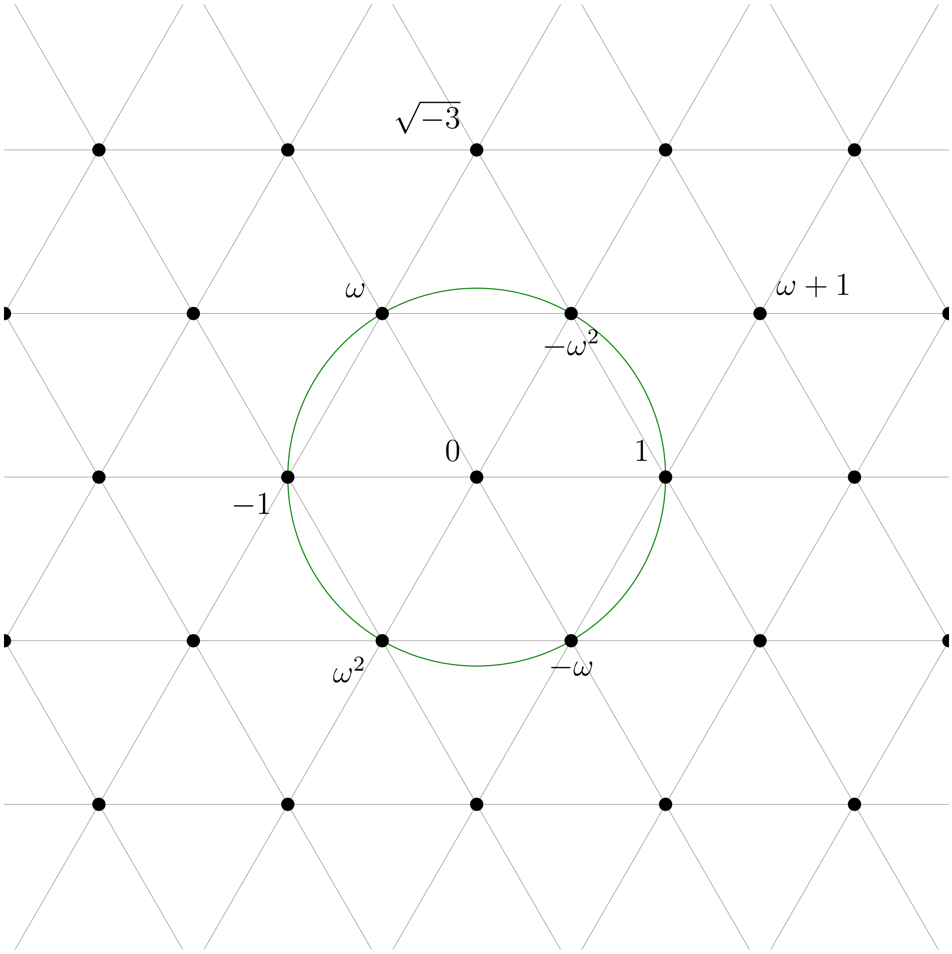
$$N : \mathbb{Z}[\omega] \to \mathbb{N}, \qquad a + b\omega \mapsto a^2 - ab + b^2 \qquad (\text{for } a, b \in \mathbb{Z})$$

is a Euclidean norm for it.

[For the sake of brevity, you are allowed to reason from a picture here.]

2.2 Hint

Geometrically speaking, the three complex numbers $1,\ \omega,\ \omega^2$ are the vertices of an equilateral triangle inscribed in the unit circle. The elements of $\mathbb{Z}[\omega]$ are the grid points of a triangular lattice that looks as follows (imagine the picture extended to infinity all on sides):



For part **(d)**, don't forget to show that $\mathbb{Z}\left[\sqrt{-3}\right]$ is a **subset** of $\mathbb{Z}[\omega]$ in the first place!

2.3 Solution

...

---

3 Exercise 3

3.1 Problem

Let R be a ring. Let M be a left R-module.

For any subset K of M, let $\operatorname{Ann} K$ denote the subset $\{r \in R \mid rk = 0 \text{ for all } k \in K\}$ of R. (This is called the *annihilator* of K.)

(a) Prove that $\operatorname{Ann} M$ is an ideal of R.

(b) Let K be any subset of M. Prove that $\operatorname{Ann} K$ is a left ideal of R. (Recall that a *left ideal* of R means a subset L of R that is closed under addition and contains 0 and satisfies $ra \in L$ for all $r \in R$ and $a \in L$.)

(c) Find an example showing that the $\operatorname{Ann} K$ in part **(b)** is not always an ideal of R.

3.2 Solution

...

---

4 Exercise 4

4.1 Problem

Let R be a ring. Let M be a left R-module. Prove the following:

(a) Let I be an ideal of R. An (I, M)*-product* shall mean a product of the form im with $i \in I$ and $m \in M$. Then,

$$IM := \{\text{finite sums of } (I, M)\text{-products}\}$$

is an R-submodule of M.

(b) Let a be a central element of R. Prove that

$$aM := \{am \mid m \in M\}$$

is an R-submodule of M.

4.2 Solution

...

---

5 Exercise 5

5.1 Problem

Let n and k be two positive integers. Let V be the subset

$$\{(a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n \mid a_1 \equiv a_2 \equiv \cdots \equiv a_n \mod k\}$$

of the $\mathbb{Z}$-module $\mathbb{Z}^n$.

It is straightforward to see that V is a $\mathbb{Z}$-submodule of $\mathbb{Z}^n$.

Show that V is free, and find a basis of V.

5.2 Solution

...

---

6 Exercise 6

6.1 Problem

Let R be any ring. Consider the map

$$\begin{aligned} S : R^{\mathbb{N}} &\to R^{\mathbb{N}}, \\ (a_0, a_1, a_2, \ldots) &\mapsto (a_0,\ a_0 + a_1,\ a_0 + a_1 + a_2,\ a_0 + a_1 + a_2 + a_3,\ \ldots) \\ &= (b_0, b_1, b_2, \ldots) \text{ where } b_i = a_0 + a_1 + \cdots + a_i. \end{aligned}$$

Consider furthermore the map

$$\begin{aligned} \Delta : R^{\mathbb{N}} &\to R^{\mathbb{N}}, \\ (a_0, a_1, a_2, \ldots) &\mapsto (a_0,\ a_1 - a_0,\ a_2 - a_1,\ a_3 - a_2,\ \ldots), \\ &= (c_0, c_1, c_2, \ldots) \text{ where } c_0 = a_0 \text{ and } c_i = a_i - a_{i-1} \text{ for all } i \geq 1. \end{aligned}$$

(a) Prove that S and Δ are R-linear maps and are mutually inverse.

(b) Recall the R-submodule

$$R^{(\mathbb{N})} = \left\{ (a_0, a_1, a_2, \ldots) \in R^{\mathbb{N}} \ \mid \ \text{only finitely many } i \in \mathbb{N} \text{ satisfy } a_i \neq 0 \right\}$$

of $R^{\mathbb{N}}$. Define a further R-submodule $R^{(\mathbb{N})+}$ of $R^{\mathbb{N}}$ by

$$R^{(\mathbb{N})+} := \left\{ (a_0, a_1, a_2, \ldots) \in R^{\mathbb{N}} \ \mid \ \text{there exists a } c \in R \text{ such that only finitely many } i \in \mathbb{N} \text{ satisfy } a_i \neq c \right\}.$$

(Thus, a sequence $(a_0, a_1, a_2, \ldots) \in R^{\mathbb{N}}$ belongs to $R^{(\mathbb{N})+}$ if and only if starting from some point on, all its entries are equal.)

Clearly, $R^{(\mathbb{N})}$ is a proper subset of $R^{(\mathbb{N})+}$ (unless R is trivial).

Prove that $R^{(\mathbb{N})} \cong R^{(\mathbb{N})+}$ as left R-modules, and in fact the restriction of the map S to $R^{(\mathbb{N})}$ is a left R-module isomorphism from $R^{(\mathbb{N})}$ to $R^{(\mathbb{N})+}$.

6.2 Solution

...