Drexel University, Department of Mathematics

Math 332: Undergraduate Abstract Algebra II, Winter 2023: Homework 5

Please solve **at most 3 of the 6 problems!**

Darij Grinberg

March 1, 2023

---

1 Exercise 1

1.1 Problem

Let R be a ring. Let I, J and K be three mutually comaximal ideals of R. Prove that $IJ + JK + KI = R$.

1.2 Hint

Expand $(i_1 + j_1)(j_2 + k_2)(k_3 + i_3)(i_4 + j_4)(j_5 + k_5)$.

Keep in mind that R need not be commutative!

1.3 Solution

...

---

2 Exercise 2

2.1 Problem

Prove that the ring

$$\mathbb{Z}\left[\sqrt{-2}\right] := \left\{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\right\}$$

is Euclidean, and that the map

$$\begin{aligned} N : \mathbb{Z}\left[\sqrt{-2}\right] &\to \mathbb{N}, \\ a + b\sqrt{-2} &\mapsto a^2 + 2b^2 \qquad (\text{for } a, b \in \mathbb{Z}) \end{aligned}$$

is a Euclidean norm for it.

2.2 Hint

Imitate the proof for $\mathbb{Z}[i]$ in Lecture 15.

2.3 Solution

...

---

3 Exercise 3

3.1 Problem

Let p be a prime such that $p \equiv 1 \mod 4$. Prove that p can be written in the form $p = x^2 + 4y^2$ for some $x, y \in \mathbb{Z}$.

3.2 Hint

No new rings are required!

3.3 Solution

...

---

4 Exercise 4

4.1 Problem

Let R be the ring $\mathbb{Z}[i]$ of Gaussian integers. Let S be the ring

$$\begin{aligned} \mathbb{Z}[2i] &= \{a + b \cdot 2i \mid a, b \in \mathbb{Z}\} \\ &= \{\text{Gaussian integers with an even imaginary part}\}. \end{aligned}$$

This ring S is a subring of R.

Define two elements $x, y \in S$ by $x = 2 + 2i$ and $y = 2 - 2i$.

(a) Find the units of S.

(b) Prove that we have $x \sim y$ in R, but we don't have $x \sim y$ in S.

(c) Prove that the ideal $xS + yS$ of S is not principal.

(d) Conclude that S is not a PID.

4.2 Hint

It may be helpful to write i' for $2i$ in order to avoid confusing i for an element of S.

For part **(c)**, argue that if $xS + yS$ was zS for some $z \in S$, then $xR + yR$ would be zR as well (why?), but this would force z to be associate to x and y in R (why?), and this would leave only four possibilities for z (why?).

4.3 Solution

...

---

5 Exercise 5

5.1 Problem

Let R be a ring, and $n \in \mathbb{N}$. Consider the left R-module R^n.

(a) Prove that the set

$$A := \{(a_1, a_2, \ldots, a_n) \in R^n \mid a_1 = a_2 = \cdots = a_n\} = \left\{ \left(\underbrace{r, r, \ldots, r}_{n \text{ times}} \right) \mid r \in R \right\}$$

is an R-submodule of R^n.

(b) Prove that the set

$$B := \{(a_1, a_2, \ldots, a_n) \in R^n \mid 1a_1 = 2a_2 = \cdots = na_n\}$$

is an R-submodule of R^n.

(c) Prove that the set

$$C := \{(a_1, a_2, \ldots, a_n) \in R^n \mid a_1 a_2 \cdots a_n = 0\}$$

is an R-submodule of R^n **only if** R is trivial or $n = 1$.

(d) Prove that the set

$$D := \{(a_1, a_2, \ldots, a_n) \in R^n \mid a_i = a_{i-1} + a_{i-2} \text{ for all } i \geq 3\}$$

is an R-submodule of R^n.

5.2 Hint

For the sake of brevity, feel free to abbreviate an n-tuple $(a_1, a_2, \ldots, a_n)$ as a.

5.3 Solution

...

---

6 Exercise 6

6.1 Problem

Let R be a ring. Let M be a left R-module. Let I be an R-submodule of M.

For any two elements $a, b \in M$, we write "$a \equiv b \mod I$" (and say that "a is congruent to b modulo I") if and only if $a - b \in I$. (This is a generalization of congruence of integers, as it is usually defined in elementary number theory. Indeed, congruence of integers modulo an integer n is recovered when $R = \mathbb{Z}$ and $I = n\mathbb{Z}$.)

Prove the following:

(a) Each $a \in M$ satisfies $a \equiv a \mod I$.

(b) If $a, b \in M$ satisfy $a \equiv b \mod I$, then $b \equiv a \mod I$.

(c) If $a, b, c \in M$ satisfy $a \equiv b \mod I$ and $b \equiv c \mod I$, then $a \equiv c \mod I$.

(d) If $a, b, c, d \in M$ satisfy $a \equiv b \mod I$ and $c \equiv d \mod I$, then $a + c \equiv b + d \mod I$.

(e) If $a, b \in M$ and $r \in R$ satisfy $a \equiv b \mod I$, then $ra \equiv rb \mod I$.

Now, we claim a sort of converse:

(f) Let us drop the requirement that I be an R-submodule of M. Instead, we require that the claims of parts **(a)**, **(c)** and **(e)** of this exercise hold. Prove that I is an R-submodule of M.

6.2 Hint

This exercise can be summarized as "modular arithmetic modulo a subset I of M works if and only if I is a submodule of M". In other words, roughly speaking, the submodules of a module M are precisely the subsets I that allow "working modulo I". This is most likely the reason why modules are called "modules"[1].

6.3 Solution

...

---

[1] The name was coined by Dedekind, although in a less general context.