Drexel University, Department of Mathematics

Math 332: Undergraduate Abstract Algebra II, Winter 2025: Homework 6

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

Darij Grinberg

February 16, 2025

1 Exercise 1

1.1 Problem

Let R be any ring. Let n be a positive integer. Let U be the subset

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

of the left R-module R^n.

It is straightforward to see that U is an R-submodule of R^n.

Show that U is free, and prove that the $n-1$ vectors

$$\begin{aligned} &(1, -1, 0, 0, \ldots, 0), \\ &(0, 1, -1, 0, \ldots, 0), \\ &\ldots, \\ &(0, 0, \ldots, 0, 1, -1) \end{aligned}$$

(that is, the $n-1$ vectors that consist of a number of 0's, followed by a 1, followed by a -1, followed again by a number of 0's) form a basis of U.

1.2 Solution

...

---

2 Exercise 2

2.1 Problem

(a) Let X be the $\mathbb{Z}$-submodule

$$\left\{(a,b,c) \in \mathbb{Z}^3 \ \mid \ a \equiv b \mod 2 \text{ and } b \equiv c \mod 3\right\}$$

of $\mathbb{Z}^3$. Prove that X is free, and find a basis of X.

(b) Let Y be the $\mathbb{Z}$-submodule

$$\left\{(a,b,c) \in \mathbb{Z}^3 \ \mid \ a \equiv b \mod 2 \text{ and } b \equiv c \mod 3 \text{ and } c \equiv a \mod 5\right\}$$

of $\mathbb{Z}^3$. Prove that Y is free, and find a basis of Y.

2.2 Solution

...

---

3 Exercise 3

3.1 Problem

Let R be a commutative ring. Let G be a finite group. Let s be the element $\sum_{g \in G} e_g$ of the group algebra $R\left[G\right]$.

(a) Prove that $s^2 = |G| \cdot s$.

(b) If $|G| \cdot 1_R$ is invertible in R, then prove that $\dfrac{1}{|G|} s \in R\left[G\right]$ is idempotent.

3.2 Remark

Part **(b)** generalizes the idempotents z in [23wa, Section 4.1.2].

3.3 Solution

...

---

4 Exercise 4

4.1 Problem

Let $n \in \mathbb{N}$. Prove that we have $x^2 + x + 1 \mid x^{2n} + x^n + 1$ in the polynomial ring $\mathbb{Z}[x]$ if and only if $3 \nmid n$ in $\mathbb{Z}$.

4.2 Hint

First show that $x^3 \equiv 1 \mod x^2 + x + 1$ in the ring $\mathbb{Z}[x]$. Here, we are using the notation $a \equiv b \mod c$ (spoken "a is congruent to b modulo c") for $c \mid a - b$ whenever a, b, c are three elements of a commutative ring R. Congruences in R are a straightforward generalization of congruences of integers (which are known from elementary number theory), and behave just as nicely; in particular, they can be added, subtracted and multiplied.]

4.3 Solution

...

---

5 Exercise 5

5.1 Problem

Let R be any commutative ring. Let $n \in \mathbb{N}$.

(a) Find the quotient and the remainder obtained when dividing $(x+1)^n$ by x.

(b) Find the quotient and the remainder obtained when dividing x^n by $x - 1$.

(c) Find the remainder obtained when dividing $(x+1)^n$ by $x - 1$.

5.2 Hint

"Finding" a polynomial here means computing its coefficients. For instance, in part **(a)**, the coefficients of the quotient will be certain binomial coefficients. I am deliberately not asking for the quotient in part **(c)**, since I don't know a closed form for its coefficients that doesn't use summation signs.

5.3 Solution

...

---

6 Exercise 6

6.1 Problem

Let $a \in \mathbb{Z}[x]$ and $b \in \mathbb{Z}[x]$ be two polynomials, with b being nonzero. Without requiring anything about the leading coefficient of b, we don't know whether there exists a pair (q, r) of polynomials in $\mathbb{Z}[x]$ such that

$$a = qb + r \qquad \text{and} \qquad \deg r < \deg b$$

(since the conditions of the division-with-remainder theorem are not guaranteed). Nevertheless, such a pair might exist.

(a) Does such a pair exist when $a = 3x^2 + 1$ and $b = 3x - 1$?

(b) Does such a pair exist when $a = 3x^3 + 1$ and $b = 3x - 1$?

(c) Does such a pair exist when $a = 3x^2 + 2x$ and $b = 3x - 1$?

(Make sure to prove your claims!)

6.2 Solution

...

References

[23wa] Darij Grinberg, *Math 332 Winter 2023 notes: An introduction to the algebra of rings and fields*, 17 January 2025. `https://www.cip.ifi.lmu.de/~grinberg/t/23wa/23wa.pdf`