

Math 332: Undergraduate Abstract Algebra II, Winter 2023: Homework 6

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

Darij Grinberg

March 12, 2023

1 EXERCISE 1

1.1 PROBLEM

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

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

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

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

(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

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

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

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

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

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 $R[G]$.

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

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

3.2 REMARK

Part (b) generalizes the idempotents z in Section 3.1.2 (Lecture 24).

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 $x^3 \equiv 1 \pmod{x^2 + x + 1}$ in the ring $\mathbb{Z}[x]$. Here, we are using the notation $a \equiv b \pmod{c}$ (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

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

(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

...
