Drexel University, Department of Mathematics

Math 332: Undergraduate Abstract Algebra II, Winter 2023: Homework 1

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

Darij Grinberg

January 11, 2025

1 Exercise 1

1.1 Problem

(a) Without computing the integer 7^4, prove that $\overline{7}^4 = \overline{1}$ in the ring $\mathbb{Z}/10$.

(b) Find a simple rule for the k-th power $\overline{7}^k$ of the element $\overline{7}$ in the ring $\mathbb{Z}/10$. Specifically, this rule should express $\overline{7}^k$ in terms of the remainder that k leaves when divided by 4.

(c) What is the units digit of the number 7^{9999} ?

*I recommend solving as many problems as you can and wish, but I will only grade and score 3 solutions per submission (and if you submit more, I get to pick which ones I grade).
Results stated in class, and claims of previous problems (even if you did not solve these previous problems), can be used without proof. For example, in solving Problem 5, you can use the result of Problem 2 without proof.
I expect approximately the level of detail that I give in class. Purely straightforward arguments (like checking the ring axioms for a direct product of rings) need not be spelled out; I only expect a note of their necessity.

1.2 Solution

...

---

2 Exercise 2

2.1 Problem

(a) Prove that every element $x \in \mathbb{Z}/5$ satisfies $x^5 = x$ in $\mathbb{Z}/5$.

(b) In the ring $\mathbb{H}$ of Hamilton quaternions (defined in Lecture 2), compute ijk and $(1+i+j+k)^2$.

Next, recall the ring F_4 constructed in Lecture 3, with its four elements $0, 1, a, b$.

(c) Prove that $a^4 = a$ in this ring.

(d) What is b^4 ?

2.2 Solution

...

---

3 Exercise 3

3.1 Problem

Let p be a prime number, and let k be a positive integer.

(a) Prove that the only idempotent[1] elements of the ring $\mathbb{Z}/p^k$ are $\overline{0}$ and $\overline{1}$.

(b) Now assume furthermore that $p \neq 2$. Prove that the only involutive[2] elements of the ring $\mathbb{Z}/p^k$ are $\overline{1}$ and $\overline{-1}$.

3.2 Solution

...

---

[1] An element a of a ring is said to be *idempotent* if $a^2 = a$.
[2] An element a of a ring is said to be *involutive* if $a^2 = 1$.

4 Exercise 4

4.1 Problem

Let R be a ring. Prove the following:

(a) If a is an idempotent element of R, then $1 - a \in R$ is again idempotent.

(b) If a is an involutive element of R, then $-a \in R$ is again involutive.

(c) If a is an idempotent element of R, then $a^n = a$ for each positive $n \in \mathbb{N}$.

(d) If a is an idempotent element of R, then $(1 + a)^n = 1 + (2^n - 1)\, a$ for each $n \in \mathbb{N}$.

4.2 Solution

...

---

5 Exercise 5

5.1 Problem

Fix an integer m. An *m-integer* shall mean a rational number r such that there exists a $k \in \mathbb{N}$ satisfying $m^k r \in \mathbb{Z}$.

For example:

- Each integer r is an m-integer (since $m^k r \in \mathbb{Z}$ for $k = 0$).
- The rational number $\frac{5}{12}$ is a 6-integer (since $6^k \cdot \frac{5}{12} \in \mathbb{Z}$ for $k = 2$), but neither a 2-integer nor a 3-integer (since multiplying it by a power of 2 will not "get rid of" the prime factor 3 in the denominator, and vice versa[3]).
- The 1-integers are the integers (since $1^k r = r$ for all r).
- Every rational number r is a 0-integer (since $0^k r \in \mathbb{Z}$ for $k = 1$).

Let R_m denote the set of all m-integers. Prove that R_m is a subring of $\mathbb{Q}$.

5.2 Remark

The ring R_m is an example of a ring "between $\mathbb{Z}$ and $\mathbb{Q}$" (in the sense that $\mathbb{Z}$ is a subring of R_m, while R_m is a subring of $\mathbb{Q}$). Note that $R_1 = \mathbb{Z}$ and $R_0 = \mathbb{Q}$, whereas $R_2 = R_4 = R_8 = \cdots$ is the ring of all rational numbers that can be written in the form $a/2^k$ with $a \in \mathbb{Z}$ and $k \in \mathbb{N}$.

---

[3] To make this more rigorous: If we had $2^k \cdot \frac{5}{12} \in \mathbb{Z}$ for some $k \in \mathbb{N}$, then we would have $12 \mid 2^k \cdot 5$, which would entail that $3 \mid 12 \mid 2^k \cdot 5$, and thus 3 would appear as a factor in the prime factorization of $2^k \cdot 5$. But this is absurd. Hence, $2^k \cdot \frac{5}{12} \in \mathbb{Z}$ cannot hold. Similarly, $3^k \cdot \frac{5}{12} \in \mathbb{Z}$ cannot hold.

5.3 Solution

...

---

6 Exercise 6

6.1 Problem

Let $n \in \mathbb{N}$. Let R be any ring. An $n \times n$-matrix $A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} \in R^{n \times n}$ will be called *centrosymmetric* if it satisfies

$$a_{i,j} = a_{n+1-i,\ n+1-j} \qquad \text{for all } i, j \in \{1, 2, \ldots, n\}.$$

(Visually, this means that A is preserved under "180°-rotation", i.e., that any two cells of A that are mutually symmetric across the center of the matrix have the same entry. For example, a centrosymmetric 4×4-matrix has the form $\begin{pmatrix} a & b & c & d \\ e & f & g & h \\ h & g & f & e \\ d & c & b & a \end{pmatrix}$ for $a, b, \ldots, h \in R$.)

Prove that the set $\{$all centrosymmetric $n \times n$-matrices with entries in $R\}$ is a subring of $R^{n \times n}$.

[**Hint:** This can be done in a particularly slick way as follows: Let W be the $n \times n$-matrix obtained from the identity matrix I_n by a horizontal reflection (or, equivalently, a vertical reflection). For example, if $n = 4$, then $W = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$. Now, show that an $n \times n$-matrix A is centrosymmetric if and only if it satisfies $AW = WA$.]

6.2 Solution

...

---

7 Exercise 7 (bonus)

7.1 Problem

There is a certain ring F_8 consisting of eight distinct elements $0, 1, a, b, c, d, e, f$. Its addition $+$ and its multiplication $\cdot$ are given by the following tables:

$x + y$	$y = 0$	$y = 1$	$y = a$	$y = b$	$y = c$	$y = d$	$y = e$	$y = f$
$x = 0$	0							
$x = 1$		0						
$x = a$		b	0					
$x = b$		a	1					
$x = c$		d	e		0			
$x = d$		c	f		1			
$x = e$		f	c		a			
$x = f$		e	d		b			

$x \cdot y$	$y = 0$	$y = 1$	$y = a$	$y = b$	$y = c$	$y = d$	$y = e$	$y = f$
$x = 0$								
$x = 1$		1						
$x = a$		a	c					
$x = b$		b						
$x = c$		c	b					
$x = d$								
$x = e$								
$x = f$								

.

Oops, I lost most of the entries! Reconstruct all missing entries in the tables. (You can take it for granted that F_8 really is a ring.)

7.2 Solution

...