1 Matrices with integer entries

Definition 1. Consider the set

$$\mathrm{Mat}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z} \right\}$$

of 2×2 matrices with integer entries. It forms a (non-commutative) ring with unity under the usual matrix addition and matrix multiplication. The unity of $\mathrm{Mat}_2(\mathbb{Z})$ is the identity matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and the zero element is the zero matrix $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

For each of the following subsets S of $\mathrm{Mat}_2(\mathbb{Z})$, answer whether S is a subring of $\mathrm{Mat}_2(\mathbb{Z})$. (Answer **Yes/ No**)

If you claim S is not a subring, specify which subring conditions are not satisfied (S doesn't contain the zero element; S is not closed under ring addition; S is not closed under ring negation; S is not closed under ring multiplication)

(a) S is the subset of $\mathrm{Mat}_2(\mathbb{Z})$ consisting of matrices with determinant 1.

> **Solution:** S is not a subring. It is closed under ring multiplication, however it fails the other three properties: S doesn't contain the zero element; S is not closed under ring addition; and S is not closed under ring negation.

(b) S is the subset of $\mathrm{Mat}_2(\mathbb{Z})$ consisting of matrices with even entries.

> **Solution:** Yes, S is a subring. (It is a ring without unity, but it's still a ring.)

(c) $S = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{Z} \right\}$ is the subset of upper-triangular matrices in $\mathrm{Mat}_2(\mathbb{Z})$.

> **Solution:** Yes, S is a subring with unity

(d) $S = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$

> **Solution:** Yes, S is a subring with unity

2 Units

Definition 2. Let R be a ring which has unity denoted by the symbol $\mathbf{1}$. An element $u \in R$ is called a *unit* (also called an *invertible element*) if there exists $v \in R$ such that $uv = vu = \mathbf{1}$.

What are the units (if any) in the ring $\mathbb{Z}_{12}$?

(Hint: Example 3.11 in Section 3.2 Groups: Definitions and Examples computes the units for $\mathbb{Z}_8$.)

Solution: The units are the nonzero elements which are relatively prime to 12:

$$1, 5, 7, 11$$

A notation that we have used all semester for this set of units is $U(12)$.

3 Fields

Use the definition and choose examples from class notes or Textbook's Section 16.2 or Section 16.1.

(a) Write the definition of a field.

(b) Give an example of an infinite field.

Solution: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

(c) Give an example of a field consisting of 29 elements.

Solution: See Example 16.17 Textbook's Section 16.2. For each prime p, the ring $\mathbb{Z}_p$ is a field.

4 Nilpotent elements

Definition 3. A ring element x is called *nilpotent* if $x^k = \mathbf{0}$ for some positive integer k.

What are the nilpotent elements (if any) in the ring $\mathbb{Z}_{12}$?

Solution: In order for x^k to be zero in $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, the integer x^k must be a multiple of $12 = 2^2 \cdot 3$, so x itself must be divisible by 2 and by 3.
The only nilpotent elements in $\mathbb{Z}_{12}$ are 0 and 6.

5 Question

(a) Let R be a ring with unity $\mathbf{1}$ and $x \in R$. Prove the following: if $x^3 = \mathbf{0}$ then $\mathbf{1} - x$ is a unit.

(Hint: Divide $1 - x^3$ by $1 - x$)

Solution: Let $v = \mathbf{1} + x + x^2$. Then we have

$$\begin{aligned}
(\mathbf{1} - x)v &= (\mathbf{1} - x)(\mathbf{1} + x + x^2) \\
&= \mathbf{1} + x + x^2 - x(\mathbf{1} + x + x^2) \\
&= \mathbf{1} + x + x^2 - x - x^2 - x^3 \\
&= \mathbf{1} - x^3 \\
&= \mathbf{1} \text{ since } x^3 = \mathbf{0}
\end{aligned}$$

(b) Let R be a ring with unity $\mathbf{1}$ and let n be a positive integer. Is the following statement true or false? (Answer **True/ False**)

$$\text{If } x \in R \text{ and } x^n = \mathbf{0}, \text{ then } \mathbf{1} - x \text{ is a unit.}$$

If you selected False, give a counterexample; otherwise, prove it in your own notebook.

Solution: True

$$\begin{aligned}(\mathbf{1} - x)(\mathbf{1} + x + x^2 + ... + x^{n-1}) &= \mathbf{1} + x + x^2 + ... + x^{n-1} - x(\mathbf{1} + x + x^2 + ... + x^{n-1}) \\ &= \mathbf{1} - x^n \\ &= \mathbf{1} \text{ since } x^n = \mathbf{0}\end{aligned}$$

6 Zero divisors

(a) Write down the definition of a *zero divisor.* (Use class notes or Textbook's Section 16.2 or Section 16.1)

(b) What are the zero divisors (if any) of the ring $\mathbb{Z}[i]$ of the Gaussian integers?
(See class notes/ Example 16.12 of Textbook's Sec 16.2)

Solution: There are no zero divisors.

(c) What are the zero divisors (if any) of the ring $\mathbb{Z}_{12}$?

Solution: All the nonzero elements which are not units: 2,3,4,6,8,9,10. For example, 9 is a zero divisor because $(9)(4) = 0$.

7 Cancellation law in an integral domain

Suppose R is an integral domain and $x \in R$. If $x^2 = x$, what are the possible values of x?
(Hint: Review the "Cancellation law for integral domains' in Week 10 class notes or Proposition 16.15 in Textbook's Section 16.2)

Solution: Suppose $x^2 = x$. Then $xx = x1$. If x is nonzero, then the cancellation law of integral domain tells us that $x = 1$.

Conclusion: $\boxed{x \text{ can either be the zero element or the unity element}}$.

8 Idempotents

Definition 4. Let R be a ring. An element x in R is called an *idempotent* if it satisfies $x^2 = x$.

What are the idempotents in $\mathbb{Z}_{12}$? (Hint: For each of the elements r in $\mathbb{Z}_{12}$, simply check whether $r^2 = r$.)

Solution: The idempotents in $\mathbb{Z}_{12}$ are $\boxed{0, 1, 4, 9}$. The computation is below:

0 is an idempotent, since $0^2 = 0$

1 is an idempotent, since $1^2 = 1$

2 is not an idempotent, since $2^2 = 4 \neq 2$

3 is not an idempotent, since $3^2 = 9 \neq 3$

4 is an idempotent, since $4^2 = 4$

5 is not an idempotent, since $5^2 = 1 \neq 5$

6 is not an idempotent, since $6^2 = 0 \neq 6$

7 is not an idempotent, since $7^2 = 1 \neq 7$

8 is not an idempotent, since $8^2 = 4 \neq 8$

9 is an idempotent, since $9^2 = 9$

10 is not an idempotent, since $10^2 = 4 \neq 10$

11 is not an idempotent, since $11^2 = 1 \neq 11$

9 Characteristic of a ring

(a) Write down the definition of the *characteristic* of a ring. (Use class notes or Textbook's Section 16.2)

(b) Write down the statement and proof of Lemma 16.18 from Textbook's Section 16.2

(c) What is the characteristic of the ring $\mathbb{Z}[i]$ of the Gaussian integers?

(d) What is the characteristic of the ring $\mathbb{Z}_{12}$? What is the characteristic of the ring $\mathbb{Z}_{625}$?

Solution: The order of the unity element 1 is 12, so the characteristic of $\mathbb{Z}_{12}$ is 12.

Solution: The order of the unity element 1 is 625, so the characteristic of $\mathbb{Z}_{625}$ is 625.

10 Acknowledgements

Write down everyone who contributed to your thought process. Write down Judson's textbook, class notes, and other written sources you used as well.