Introduction to Abstract Algebra II: Homework 1

Due on January 14, 2026 at 23:59

Victor Ostrik 10:00

Hashem A. Damrah
UO ID: 952102243

Exercise 22.12. Decide whether the set $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ with the usual addition and multiplication are defined (closed), and give a ring structure. If a ring is not formed, tell why this is the case. If a ring is formed, state whether the ring is commutative, whether it has unity, and whether it is a field.

Solution. Let $x, y \in A = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Adding them, we have

$$x + y = (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in A..$$

Multiplying them, we have

$$x \cdot y = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in A..$$

Therefore, A is closed under addition and multiplication.

Since addition and multiplication of integers are associative and commutative, the same properties hold for A. The additive identity is $0 + 0\sqrt{2}$, and the multiplicative identity is $1 + 0\sqrt{2}$. The additive inverse of $a + b\sqrt{2}$ is $-a - b\sqrt{2}$, which is also in A. Thus, A forms a commutative ring with unity. However, A is not a field because not every non-zero element has a multiplicative inverse. □

Exercise 22.18. Describe all the units of the ring $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$.

Solution. The units of the ring $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$ are the elements (a, b, c) such that a and c are units in $\mathbb{Z}$ and b is a unit in $\mathbb{Q}$. The only units in $\mathbb{Z}$ are 1 and -1, while every non-zero element in $\mathbb{Q}$ is a unit. Therefore, the units of the ring $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$ are of the form $(\pm 1, b, \pm 1)$ where $b \in \mathbb{Q}^*$. □

Exercise 22.20. Consider the matrix ring $M_2(\mathbb{Z}_2)$.

(i) Find the *order* of the ring, that is, the number of elements in it.

(ii) List all units in the ring.

Solution to (i). Each entry in each 2×2 matrix has 2 possible options, either 0 or 1. Since there are 4 slots, each with 2 options, the total number of matrices is $2^4 = 16$. Therefore, the order of the ring $M_2(\mathbb{Z}_2)$ is 16. □

Solution to (ii). A matrix in $M_2(\mathbb{Z}_2)$ is a unit if its determinant is 1 in $\mathbb{Z}_2$. The determinant of a 2×2 matrix is given by $ad - bc$. Meaning that either $ad = 1$ and $bc = 0$, or $ad = 0$ and $bc = 1$. For the first case, when $ad = 1$ and $bc = 0$, we have the following matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

For the second case, when $ad = 0$ and $bc = 1$, we have the following matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Therefore, the units in the ring $M_2(\mathbb{Z}_2)$ are

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$ □

Exercise 22.21. If possible, give an example of a homomorphism $\varphi : R \to R'$ where R and R' are rings with unity $1 \neq 0$ and $1' \neq 0'$, and where $\varphi(1) \neq 0'$ and $\varphi(1) \neq 1'$.

Solution. Assume we have an isomorphism $\varphi : R \to R'$ such that $\varphi(1) \neq 0'$ and $\varphi(1) \neq 1'$. Since φ is a homomorphism, we have

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot' \varphi(1).$$

This implies that $\varphi(1)$ is an idempotent element in R'. However, in a ring with unity, the only idempotent elements are $0'$ and $1'$. Therefore, this isn't possible. $\square$

Exercise 22.26. How many homomorphisms are there of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ into $\mathbb{Z}$?

Solution. Assume $\varphi : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is a homomorphism. Then, it must send the unity element $(1, 1, 1)$ to the unity element 1 in $\mathbb{Z}$. Therefore,

$$\varphi(1, 1, 1) = \varphi(1, 0, 0) + \varphi(0, 1, 0) + \varphi(0, 0, 1) = 1.$$

Let $\mathbf{e}_1 = (1, 0, 0)$, $\mathbf{e}_2 = (0, 1, 0)$, and $\mathbf{e}_3 = (0, 0, 1)$. Therefore, there are three possible homomorphisms defined by

$$\begin{aligned}
\varphi_1 :& \quad \varphi_1(\mathbf{e}_1) = 1, \quad \varphi_1(\mathbf{e}_2) = 0, \quad \varphi_1(\mathbf{e}_3) = 0 \\
\varphi_2 :& \quad \varphi_2(\mathbf{e}_1) = 0, \quad \varphi_2(\mathbf{e}_2) = 1, \quad \varphi_2(\mathbf{e}_3) = 0 \\
\varphi_3 :& \quad \varphi_3(\mathbf{e}_1) = 0, \quad \varphi_3(\mathbf{e}_2) = 0, \quad \varphi_3(\mathbf{e}_3) = 1.
\end{aligned}$$

These $\mathbf{e}_i$ elements form a complete set of orthogonal idempotent elements. This means that they satisfy the following properties

$$\mathbf{e}_i\mathbf{e}_j = \delta_{ij}\mathbf{e}_i \quad \text{and} \quad \sum_{i=1}^{3} \mathbf{e}_i = 1.$$

This is clearly satisfied by our choice of $\mathbf{e}_i$ elements, i.e.,

$$f(\mathbf{e}_i)f(\mathbf{e}_j) = \delta_{ij}f(\mathbf{e}_i) \quad \text{and} \quad f(\mathbf{e}_1) + f(\mathbf{e}_2) + f(\mathbf{e}_3) = 1.$$

Therefore, there are exactly 3 homomorphisms from $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ into $\mathbb{Z}$. $\square$

Exercise 22.28. Find all solutions of the equation $x^2 + x - 6 = 0$ in the ring $\mathbb{Z}_{14}$ by factoring the quadratic polynomial. Compare with Exercise 27.

Solution. Factoring the equation $x^2 + x - 6 = 0$, we have $(x + 3)(x - 2) = 0$. So, we clearly have the solutions $x = -3$ and $x = 2$. But $x = -3$ is equivalent to $x = 11$ in $\mathbb{Z}_{14}$. Notice that for $x = 4$, we have

$$(4 + 3)(4 - 2) = 7 \cdot 2 = 14 \equiv 0 \pmod{14}.$$

Thus, $x = 4$ is another solution in the ring $\mathbb{Z}_{14}$. We also have for $x = 9$,

$$(9 + 3)(9 - 2) = 12 \cdot 7 = 84 \equiv 0 \pmod{14}.$$

Therefore, all the solutions to the equation $x^2 + x - 6 = 0$ in the ring $\mathbb{Z}_{14}$ are $x = 2$, 4, 9, and 11. $\square$

Exercise 22.39. Show that if U is the collection of all units in a ring $\langle R, +, \cdot\rangle$ with unity, then $\langle U, \cdot\rangle$ is a group. [*Warning:* Be sure to show that U is closed under multiplication.]

Solution. Assume that R is a ring with unity $1 \neq 0$. Then, clearly U is non-empty since it contains at least the unity element 1. Let $a, b \in U$. Then, $ab \in U$, since there exists a^{-1}, b^{-1} such that

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1.$$

Therefore, U is closed under multiplication. Also, multiplication in R is associative, so it is associative in U. The unity element 1 is in U and serves as the identity element. Finally, for each $a \in U$, there exists an inverse $a^{-1} \in U$. Therefore, $\langle U, \cdot\rangle$ is a group. $\square$

Exercise 22.40. Show that $a^2-b^2=(a+b)(a-b)$ for all a and b in a ring R if and only if R is commutative.

Solution. Assume $a^2-b^2=(a+b)(a-b)$ for all $a,b\in R$. Expanding, we have

$$a^2-b^2=a^2-ab+ba-b^2.$$

Adding b^2-a^2 to both sides, we have $0=-ab+ba$, which implies that $ab=ba$ for all $a,b\in R$. Therefore, R is commutative.

Conversely, assume R is commutative. Then, for all $a,b\in R$, we have

$$(a+b)(a-b)=a^2-ab+ba-b^2=a^2-ab+ab-b^2=a^2-b^2.$$

Therefore, $a^2-b^2=(a+b)(a-b)$ for all $a,b\in R$. □

Exercise 22.42. Show that the rings $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic. Show that the fields $\mathbb{R}$ and $\mathbb{C}$ are not isomorphic.

Solution. Assume there exists an isomorphism $\varphi: 2\mathbb{Z}\to 3\mathbb{Z}$. Then, we have

$$\varphi(2)=\varphi(1\cdot 2)=\varphi(1)\cdot'\varphi(2),$$

where $\cdot$ is the multiplication in $2\mathbb{Z}$ and $\cdot'$ is the multiplication in $3\mathbb{Z}$. Since $\varphi(1)\in 3\mathbb{Z}$, we can write $\varphi(1)=3k$ for some $k\in\mathbb{Z}$. Therefore,

$$\varphi(2)=(3k)\cdot'\varphi(2)=3k\cdot\varphi(2).$$

This implies that $\varphi(2)$ is divisible by 3. However, 2 is not divisible by 3, which contradicts the fact that φ is an isomorphism. Therefore, $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic.

Assume that there exists an isomorphism $\varphi:\mathbb{R}\to\mathbb{C}$. Then, we have

$$\varphi(1)=\varphi(1\cdot 1)=\varphi(1)\cdot'\varphi(1).$$

This implies that $\varphi(1)$ is an idempotent element in $\mathbb{C}$. The only idempotent elements in $\mathbb{C}$ are 0 and 1. Since $\varphi(1)\neq 0$, we have $\varphi(1)=1$. Now, consider the element $i\in\mathbb{C}$, where $i^2=-1$. Since φ is surjective, there exists $r\in\mathbb{R}$ such that $\varphi(r)=i$. Then, we have

$$\varphi(r^2)=\varphi(r)\cdot'\varphi(r)=i\cdot' i=-1.$$

However, there is no real number r such that $r^2=-1$. This contradicts the fact that φ is an isomorphism. Therefore, $\mathbb{R}$ and $\mathbb{C}$ are not isomorphic. □

Exercise 22.43. Let p be a prime. Show that in the ring $\mathbb{Z}_p$ we have $(a+b)^p=a^p+b^p$ for all $a,b\in\mathbb{Z}_p$. [*Hint:* Observe that the usual binomial expansion $(a+b)^n$ is valid in a *commutative ring*.]

Solution. In a commutative ring, the binomial expansion states that

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k.$$

Applying this to our case with $n=p$, we have

$$(a+b)^p=\sum_{k=0}^{p}\binom{p}{k}a^{p-k}b^k.$$

Since p is a prime, the binomial coefficients $\binom{p}{k}$ for $1\le k\le p-1$ are all divisible by p. Therefore, in the ring $\mathbb{Z}_p$, these coefficients are equivalent to 0. Thus, the only terms that survive in the sum are those for $k=0$ and $k=p$. Hence, we have

$$(a+b)^p=\binom{p}{0}a^pb^0+\binom{p}{p}a^0b^p=a^p+b^p.$$

Therefore, in the ring $\mathbb{Z}_p$, we have $(a+b)^p=a^p+b^p$ for all $a,b\in\mathbb{Z}_p$. □