Modern Algebra HW 8

Michael Nameika

November 2022

Section 18 Problems

Decide whether the indicated operations of addition and multiplication are defined (closed) on the set, and give a ring structure.

Problem 12 $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ with the usual addition and multiplication.
Let $S = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. I claim that $\langle S, +, \cdot\rangle$ forms a field.
Proof: To begin, we must show that $\langle S, +\rangle$ is an abelian group. To do so, we must first show S is closed under addition. Well, let $\alpha, \beta \in S$ be defined as $\alpha = a_1 + b_1\sqrt{2}$ and $\beta = a_2 + b_2\sqrt{2}$ for the remainder of the proof and consider $\alpha + \beta$:

$$\begin{aligned}\alpha + \beta &= a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2}\\ &= (a_1 + a_2) + (b_1 + b_2)\sqrt{2}\end{aligned}$$

By closure of $\mathbb{Q}$, we have $a_1 + a_2 \in \mathbb{Q}$ and $b_1 + b_2 \in \mathbb{Q}$, so $\alpha + \beta \in S$. Now, by associativity of addition in $\mathbb{Q}$, we have that U is associative under $+$. Now, we must show that there exists an identity element. I claim that $e_+ = 0 + 0\sqrt{2}$ is the identity element of S under addition. Consider $e_+ + \alpha$:

$$\begin{aligned}e_+ + \alpha &= 0 + 0\sqrt{2} + a_1 + b_1\sqrt{2}\\ &= a_1 + b_1\sqrt{2}\\ &= a_1 + b_1\sqrt{2} + 0 + 0\sqrt{2}\\ &= \alpha\end{aligned}$$

Now we must show that every element $\alpha \in U$ there exists some $\alpha^{-1} \in S$ such that $\alpha + \alpha^{-1} = \alpha^{-1} + \alpha = e_+$. I claim that for α defined above, we have $\alpha^{-1} = -a_1 - b_1\sqrt{2}$. Consider the following:

$$\begin{aligned}\alpha + \alpha^{-1} &= a_1 + b_1\sqrt{2} + (-a_1 - b_1\sqrt{2})\\ &= a_1 - a_2 + (b_1 - b_2)\sqrt{2}\\ &= 0 + 0\sqrt{2} = e_+\\ &= -a_2 - b_2\sqrt{2} + a_1 + b_1\sqrt{2}\\ &= \alpha^{-1} + \alpha\end{aligned}$$

Thus, $\langle S, +\rangle$ forms a group. Additionally, by commutativity of addition in $\mathbb{Q}$, we have $\langle S, +\rangle$ is an abelian group. Now we must show that $\langle S^{\neq 0}, \cdot\rangle$ is a group. To begin, we must show that $S^{\neq 0}$ is closed under multiplication. Consider $\alpha \cdot \beta$:

$$\begin{aligned}\alpha \cdot \beta &= (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) \\ &= a_1a_2 + 2b_1b_2 + a_1b_2\sqrt{2} + a_2b_1\sqrt{2} \\ &= (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}\end{aligned}$$

By closure of $\mathbb{Q}$, we have $a_1a_2 + 2b_1b_2 \in \mathbb{Q}$ and $a_1b_2 + a_2b_1 \in \mathbb{Q}$. Thus, $\alpha \cdot \beta \in S$, so S is closed under multiplication. Now we must show that associativity holds for S. This holds by associativity of $\mathbb{Q}$. Now we must show that there exists an identity element in S.

I claim that $e = 1 + 0\sqrt{2} \in U$ is the identity. Well, let $\alpha = a_1 + b_1\sqrt{2} \in U$ and consider $e \cdot \alpha$:

$$\begin{aligned}e \cdot \alpha &= (1 + 0\sqrt{2}) \cdot (a_1 + b_1\sqrt{2}) \\ &= a_1 + b_1\sqrt{2} \\ &= (a_1 + b_1\sqrt{2}) \cdot (1 + 0\sqrt{2}) \\ &= \alpha \cdot e \\ &= \alpha\end{aligned}$$

So e is the identity for $\langle U, \cdot\rangle$. Now we must show that for every $\alpha \in U$, there exists $\alpha^{-1} \in U$ such that $\alpha^{-1} \cdot \alpha = \alpha \cdot \alpha^{-1} = e$. Let $\alpha = a_1 + b_1\sqrt{2} \in U$. I claim that $\alpha^{-1} = 1/(a_1 + b_1\sqrt{2})$. Well,

$$\begin{aligned}\frac{1}{a_1 + b_1\sqrt{2}} &= \left(\frac{1}{a_1 + b_1\sqrt{2}}\right)\left(\frac{a_1 - b_1\sqrt{2}}{a_1 - b_1\sqrt{2}}\right) \\ &= \frac{a_1 - b_1\sqrt{2}}{a_1^2 - 2b_1^2} \\ &= \frac{a_1}{a_1^2 - 2b_1^2} - \frac{b_1}{a_1 - 2b_1^2}\sqrt{2}\end{aligned}$$

Now, for all $a_1, b_1 \in \mathbb{Q}$, we cannot have $a_1^2 = 2b_1^2$ (notice that this would give us that $\sqrt{2} \in \mathbb{Q}$ since we would get $a_1/b_1 = \sqrt{2}$), so $a_1/(a_1^2 - 2b_1), -b_1/(a_1^2 - 2b_1^2) \in \mathbb{Q}$, so $\alpha^{-1} \in S^{\neq 0}$. Thus, $\langle S^{\neq 0}, \cdot\rangle$ forms a group. Finally, we have established that $\langle S, +, \cdot\rangle$ forms a field.

37. 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.

Proof: Let $\langle U, \cdot\rangle$ be the collection of all units in a ring $\langle R, +, \cdot\langle$. We must show that $\langle U, \cdot\rangle$ is a group. To begin, we must show $\langle U, \cdot\rangle$ is closed under multiplication. Let $a, b \in U$ and consider $a \cdot b$. Let $c = a \cdot b$ and notice

$$\begin{aligned}c \cdot b^{-1} &= a \cdot b \cdot b^{-1} \\ c \cdot b^{-1} &= a \\ c \cdot b^{-1} \cdot a^{-1} &= a \cdot a^{-1} \\ c \cdot b^{-1} \cdot a^{-1} &= e\end{aligned}$$

where e is the identity in U. That is, we have

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

and since $b^{-1}, a^{-1} \in R$, so $b^{-1} \cdot a^{-1} \in R$, and so $a \cdot b$ is a unit in U. Thus, U is closed under multiplication. Now we must show that associativity holds. Since $U \subseteq R$, we have for any $a, b, c \in U$, $a, b, c \in R$, so associativity comes immediately from the fact that $\langle R, +, \cdot \rangle$ is a ring. Now we must show there exists an identity element. Well, since R is a ring with unity, call the unity element 1_R. Notice that $1_R \cdot 1_R = 1_R$, so 1_R is a unit in R. That is, $1_R \in U$. Thus, 1_R is the identity of U. Finally, we must show that for every $a \in U$. there exists an inverse element a^{-1} such that $a \cdot a^{-1} = a^{-1} \cdot a = 1_R$. Well, since U is a set of units in R, we get this for free! Thus, $\langle U, \cdot \rangle$ is a group.

41. (Freshman exponentiation) Let p be a prime. Show that in the ring $\mathbb{Z}_p$ we have $(a+b)^p = a^p + b^p$ for all $a, b \in \mathbb{Z}_p$. Also, is this result true in $\mathbb{Z}_6$?

Proof: To begin, recall the binomial theorem:

$$(a+b)^p = \sum_{k=1}^{n} \binom{n}{k} a^{p-k} b^k$$

Expanding out a few terms, we see

$$\sum_{k=1}^{n} \binom{n}{k} a^{p-k} b^k = \binom{n}{0} a^p + \binom{n}{1} a^{p-1} b + \cdots + \binom{n}{n-1} a b^{p-1} + \binom{n}{n} b^p$$

Notice for all the terms $\binom{n}{l}$ contain a factor of p in the numerator for $0 < l < n$, so $\binom{n}{l} = 0 \mod p$. That is, we are left with

$$\sum_{k=1}^{n} \binom{n}{k} a^{p-k} b^k = a^p + b^p$$

This result does not hold in $\mathbb{Z}_6$. Let $a = b = 2$ and first consider $(a+b)^6$:

$$\begin{aligned}(a+b)^p &= (2+2)^6 \\ &= 4^6 \\ &= (2^3)^4 \\ &= 2^4 \\ &= 4\end{aligned}$$

Now consider $a^p + b^p$:

$$\begin{aligned}a^p + b^p &= 2^6 + 2^6 \\ &= (2^3)^2 + (2^3)^2 \\ &= 2^2 + 2^2 \\ &= 4 + 4 \\ &= 2 \\ &\neq (a+b)^p\end{aligned}$$

Section 19 Problems

3. Find all solutions of the equation $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_6$.

Notice that we can factor $x^2 + 3x + 2$ as

$$x^2 + 3x + 2 = (x+2)(x+1)$$

so our "obvious" solutions are $x = -2 \equiv 4 \mod 6$ and $x = -1 \equiv 5 \mod 6$. Now, let us try the remaining elements of $\mathbb{Z}_6$ to see if they work:

$$\begin{aligned} x = 1: &\quad (1+2)(1+1) = (3)(2) = 6 \equiv 0 \mod 6 \\ x = 2: &\quad (2+2)(2+1) = (4)(3) = 12 \equiv 0 \mod 6 \\ x = 3: &\quad (3+2)(3+1) = (5)(4) = 20 \equiv 2 \mod 6 \end{aligned}$$

So we can see the solutions to this equation in $\mathbb{Z}_6$ are $x = 1, 2, 4, 5$.

23. An element a of a ring R is **idempotent** if $a^2 = a$. Show that an integral domain contains exactly two idempotent elements.

Proof: Let R be an integral domain. We wish to show that R has exactly two idempotent elements. To begin, the zero element of R is idempotent:

$$0 \cdot 0 = 0$$

Additionally, since R is an integral domain, R has a unity element, call it 1_R, and 1_R is an idempotent:

$$1_R \cdot 1_R = 1_R$$

Now we must show that there exist no other idempotent elements. Suppose by way of contradiction that there exists another idempotent element $a \in R$, $a \neq 0, 1_R$. Then

$$a^2 = a$$

but since R is an integral domain, a has a multiplicative inverse and cancellation holds, so

$$\begin{aligned} \frac{1}{a}a^2 &= \frac{1}{a}a \\ a &= 1_R \end{aligned}$$

contradicting our assumption that $a \neq 1_R$. Thus, an integral domain contains exactly two idempotent elements.