CS21201 Discrete Structures

Practice Problems

Abstract Algebraic Structures

1. Define two operations on $\mathbb{Z}$ as

$$a \oplus b = a + b + u,$$
$$a \odot b = a + b + vab,$$

where u, v are constant integers. For which values of u and v, is $(\mathbb{Z}, \oplus, \odot)$ a ring?

Solution [*Additive axioms*] $\oplus$ is clearly commutative. For associativity, we note that $(a \oplus b) \oplus c = (a+b+u) \oplus c = a+b+c+2u$, whereas $a \oplus (b \oplus c) = a \oplus (b+c+u) = a+b+c+2u$, that is, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ irrespective of u. The additive identity is $-u$, because $a \oplus (-u) = a + (-u) + u = a$ and $(-u) \oplus a = (-u) + a + u = a$. Finally, $a + (-2u - a) + u = (-2u - a) + a + u = -u$, so $-2u - a$ is the additive inverse of a. In short, the additive axioms do not impose any constraints on u (and v is not involved in this addition).

[*Multiplicative axioms*] We have $(a \odot b) \odot c = (a + b + vab) \odot c = a + b + vab + c + v(a + b + vab)c = a+b+c+v(ab+ac+bc+abc)$, whereas $a \odot (b \odot c) = a \odot (b+c+vbc) = a+(b+c+vbc)+va(b+c+vbc) = a+b+c+v(ab+ac+bc+abc)$, so $\odot$ is associative for any value of v. Although not needed in a general ring, this multiplication is commutative and has the identity 0. Again, no conditions on v (and u) are imposed.

[*Distributivity*] Because of commutativity, it suffices to look only at $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$, that is, $a \odot (b+c+u) = (a+b+vab) \oplus (a+c+vac)$, that is, $a + (b+c+u) + va(b+c+u) = (a+b+vab) + (a + c + vac) + u$, that is, $a+b+c+u+vab+vac+uva = 2a+b+c+u+vab+vac$, that is, $uva = a$. Since this must hold for all integers a, we must have $uv = 1$.

The only possibilities are therefore $u = v = 1$ and $u = v = -1$.

2. Take $u = v = 1$ is Exercise 1.

(a) Find the units of $(\mathbb{Z}, \oplus, \odot)$. Find their respective inverses.

Solution The multiplicative identity is 0. So $a \odot b = 0$ (with $a \neq -1$) implies $a + b + ab = 0$, that is, $b(a+1) = -a$, that is, $b = -\left(\frac{a}{a+1}\right)$. This b is an integer if and only if $a = 0$ or $a = -2$. The inverse of 0 is 0, and of -2 is -2.

(b) Prove that the set of all odd integers is a subring of this ring. What about the set of all even integers?

Solution It suffices to verify that $a \ominus b$ and $a \odot b$ are odd if a, b are odd. The additive inverse of b is $-2u - b = -2 - b$, which is odd if a is odd. But then, $a \ominus b = a \oplus (-2-b) = a - 2 - b + 1 = a - b - 1$ is odd if a, b are odd. Also, $a \odot b = a + b + ab$ is odd if a, b are odd.

Even integers do not constitute a subring, because closure of $\oplus$ does not hold.

3. Let $\mathbb{Z}_1$ be the ring of Exercise 1 with $u = v = 1$, and $\mathbb{Z}_2$ the ring of Exercise 1 with $u = v = -1$. Define a ring isomorphism $\mathbb{Z}_1 \to \mathbb{Z}_2$.

Solution Consider the map $f : \mathbb{Z}_1 \to \mathbb{Z}_2$ as $f(a) = -a$. Then, $f(a \oplus_1 b) = f(a + b + 1) = -(a + b + 1)$, whereas $f(a) \oplus_2 f(b) = (-a) \oplus_2 (-b) = (-a) + (-b) - 1 = -(a + b + 1)$. Moreover, $f(a \odot_1 b) = f(a + b + ab) = -(a+b+ab)$, and $f(a) \odot_2 f(b) = (-a) \odot_2 (-b) = (-a) + (-b) - (-a)(-b) = -(a+b+ab)$.

4.

Let K, L be fields, and $f : K \to L$ a non-zero ring homomorphism.

(a) Prove/disprove: $f(1_K) = 1_L$.

Solution *True*. Since f is non-zero, there exists $a \in K$ such that $f(a) \neq 0_L$. But then, $f(a) = f(a \cdot 1_K) = f(a) \cdot f(1_K)$. Since $f(a) \neq 0_L$, it is a unit, so by cancellation, we have $f(1_K) = 1_L$.

(b) Prove that f is injective.

Solution Let $f(a) = f(b)$. If $a \neq b$, then $u = a - b$ is non-zero and so a unit of K. But then, we have $1_L = f(1_K) = f(uu^{-1}) = f(u)f(u^{-1}) = f(a-b)f(u^{-1}) = (f(a) - f(b))f(u^{-1}) = 0_L \cdot f(u^{-1}) = 0_L$. By definition, a field is a non-zero ring. Therefore $0_L = 1_L$ is a contradiction.

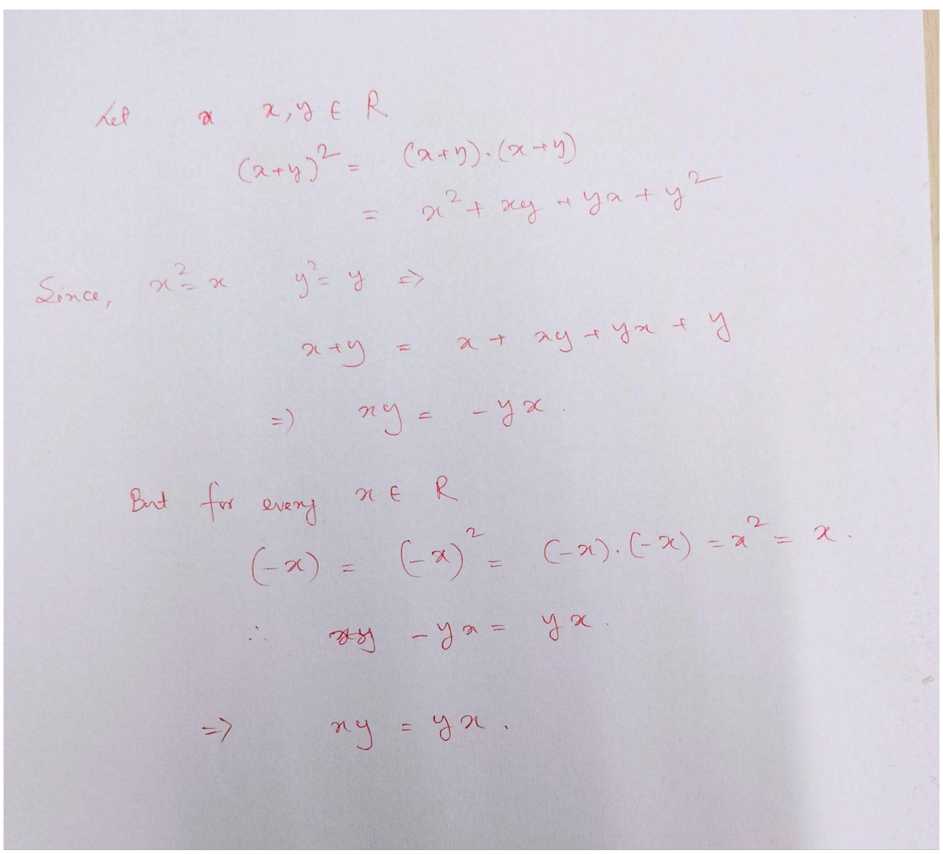
5.

What is the inverse of an element a in the group $G = \{a \in \mathbb{R} \mid a > 0\}$ under the operation $\odot$ defined by $a \odot b = a^{\ln b}$?

(A) $1/e^a$ **(B)** $1/a$ **(C)** $1/\ln a$ **(D)** $e^{1/\ln a}$

Solution The identity element x is computed from: $a^{\ln x} = a \Rightarrow x = e$. Inverse of a is computed as: $a^{\ln a^{-1}} = e \Rightarrow \ln a^{-1} \ln a = \ln e = 1 \Rightarrow a^{-1} = e^{1/\ln a}$.

6. Let (R,+,·) be a ring such that for every x ∈ R, x·x = x. Prove or disprove that R is a commutative



Let x, y ∈ R

$(x+y)^2 = (x+y)\cdot(x+y)$

$= x^2 + xy + yx + y^2$

Since, $x^2 = x$ $y^2 = y$ ⇒

$x+y = x + xy + yx + y$

⇒ $xy = -yx$.

But for every $x \in R$

$(-x) = (-x)^2 = (-x)\cdot(-x) = x^2 = x$.

∴ $-yx = yx$.

⇒ $xy = yx$.

7. Let A,B are subgroups of a group G. Prove or disprove that A∩B is also a subgroup of G.

Solution.

To solve the problem of proving whether $A \cap B$ is a subgroup of G, let A and B be subgroups of a group G. We need to check if $A \cap B$ satisfies the subgroup criteria:

1. **Closure**: For any $a, b \in A \cap B$, $ab \in A \cap B$.
2. **Identity**: The identity element $e \in G$ must be in $A \cap B$.
3. **Inverses**: For any $a \in A \cap B$, $a^{-1} \in A \cap B$.

Proof:

1. **Closure**: Since A and B are subgroups of G, for any $a, b \in A$, $ab \in A$, and for any $a, b \in B$, $ab \in B$. Therefore, for any $a, b \in A \cap B$, $ab \in A$ and $ab \in B$. Thus, $ab \in A \cap B$.
2. **Identity**: Since A and B are subgroups, the identity element $e \in G$ is in both A and B. Hence, $e \in A \cap B$.
3. **Inverses**: For any $a \in A \cap B$, since A and B are subgroups, $a^{-1} \in A$ and $a^{-1} \in B$. Therefore, $a^{-1} \in A \cap B$.

Conclusion:

Since $A \cap B$ satisfies closure, contains the identity element, and includes inverses for all its elements, $A \cap B$ is indeed a subgroup of G.

Result: $A \cap B$ is a subgroup of G.

CS21201 Discrete Structures

Tutorial 10

Abstract Algebraic Structures

1. Let R be a commutative ring with identity, and R[x] the set of univariate polynomials with coefficients from R. Define addition and multiplication of polynomials in the usual way. Prove that R[x] is an integral domain if and only if R is an integral domain.

Solution [$\Rightarrow$] Take non-zero elements $a, b \in R$. Then a and b are non-zero (constant) polynomials. Since $R[x]$ is an integral domain, ab is not the zero polynomial. But ab is again a constant polynomial. It follows that $ab \neq 0$.

[$\Leftarrow$] Suppose that there exist $A(x), B(x) \in R[x]$ such that $A(x)B(x) = 0$, $A(x) \neq 0$, and $B(x) \neq 0$. Write $A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ with $a_d \neq 0$ and $d \geqslant 0$, and $B(x) = b_0 + b_1x + b_2x^2 + \cdots + b_ex^e$ with $b_e \neq 0$ and $e \geqslant 0$. Since $A(x)B(x) = 0$, we have $a_db_e = 0$. This implies that R is not an integral domain.

2. Prove that Z[√5] ={a+b√5|a,b∈Z} is an integral domain.

Solution Closure under subtraction and multiplication is easy to check. Since $\mathbb{R}$ is commutative, $\mathbb{Z}[\sqrt{5}]$ is so too. Finally, take $a = 1$ and $b = 0$ in the definition to conclude that $\mathbb{Z}[\sqrt{5}]$ contains the multiplicative identity.

3. Let G be a (multiplicative) group, and H,K subgroups of G. Prove that H∪K is a subgroup of G if and only if H ⊆K or K ⊆H

Solution [If] Obvious.

[Only if] $H \cup K$ is a subgroup of G. Suppose that H is not contained in K. Then, there exists $h \in H$ such that $h \notin K$. Take any $k \in K$. Since h, k are both in $H \cup K$, and $H \cup K$ is a subgroup, we have $hk \in H \cup K$. Suppose that $hk \in K$. Since $k \in K$, we have $k^{-1} \in K$, so $(hk)k^{-1} = h \in K$, a contradiction. Therefore $hk \in H$. But $h \in H$, so $h^{-1} \in H$, and therefore $h^{-1}(hk) = k \in H$. It follows that $K \subseteq H$.