MTH327H LAB WORK 1 (FALL 2023)

Axioms of a number field $\mathbb{Q}$ ($\mathbb{R}$, $\mathbb{Z}_p$)

A1 $\forall a, b, c \in \mathbb{Q}$, $(a+b)+c = a+(b+c)$ (associativity);
A2 $\forall a, b \in \mathbb{Q}$, $a+b = b+a$ (commutativity);
A3 $\exists 0 \in \mathbb{Q}$ such that for any $a \in \mathbb{Q}$, $a+0 = a$;
A4 $\forall a \in \mathbb{Q}$, $\exists -a \in \mathbb{Q}$ such that $a+(-a) = 0$.

Axioms A1–A4 supply $\mathbb{Q}$ with the structure of **group** w.r.t. addition.

M1 $\forall a, b, c \in \mathbb{Q}$, $(a \cdot b) \cdot c = a] \cdot (b \cdot c)$ (associativity);
M2 $\forall a, b \in \mathbb{Q}$, $a \cdot b = b \cdot a$ (commutativity);
M3 $\exists 1 \in \mathbb{Q}$ such that for any $a \in \mathbb{Q}$, $a \cdot 1 = a$;
M4 $\forall a \neq 0 \in \mathbb{Q}$, $\exists a^{-1} \in \mathbb{Q}$ such that $a \cdot a^{-1} = 1$.

Axioms M1–M4 supply $\mathbb{Q} \backslash \{0\}$ with the structure of **group** w.r.t. multiplication.

Finally, we have the **distributive law**:

DL $\forall a, b, c \in \mathbb{Q}$, $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$.

Theorem. 1 *Axioms A1–A4 imply*

(a) *if* $a+b = a+c$ *then* $b = c$;
(b) *if* $a+b = a$ *then* $b = 0$;
(c) *if* $a+b = 0$ *then* $a = -b$;
(d) $-(-a) = a$

Proof: (a) $b = b+0 = b+(a+(-a)) = (b+a)+(-a) = (c+a)+(-a) = c+(a+(-a)) = c+0 = c$, thus proved.

(b) $a+b = a = a+0$, so by statement (a) [applied with $c = 0$], $b = c = 0$.
(c) $a+b = 0 = a+(-a)$, so by statement (a) $b = -a$.
(d) $(-a)+(-(-a)) = 0 = (-a)+a$, so, again by statement (a), $-(-a) = a$.

Team members:

Exercise 1 (Proof by induction). [A *sequence* (a_n) is an infinite ordered set of numbers a_i enumerated by natural numbers i. In general, we do not require $a_i \neq a_j$ for $i \neq j$.]

Let the sequence $(a_n) \subset \mathbb{Q}$ be defined **recursively**: $a_1 = 0$, $a_n = a_{n-1}^2 + 1/4$ for all $n \geq 2$. Prove, using induction and familiar to you relations $\geq$, $\leq$ between rational numbers, that $a_n < 1/2$ for all natural n.

Base: $a_1 = 0 < 1/2$ (check, just for curiosity next couple of terms: $a_2 = a_1^2 + \frac{1}{4} = \frac{1}{4} < \frac{1}{2}$, $a_3 = a_2^2 + \frac{1}{4} = \frac{1}{16} + \frac{1}{4} = \frac{5}{16} < \frac{1}{2}$)

Assumption $a_n < 1/2$

Implication $a_{n+1} = a_n^2 + \frac{1}{4} < \left(\frac{1}{2}\right)^2 + \frac{1}{4} = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$

thus proved

Exercise 2. Prove the theorem

Theorem 2 *Axioms M1–M4 imply*

(0) *the element* 1 *is unique!*
(a) *for* $a \neq 0$, *if* $a \cdot b = a \cdot c$ *then* $b = c$;
(b) *for* $a \neq 0$, *if* $a \cdot b = a$ *then* $b = 1$;
(c) *for* $a \neq 0$, *if* $a \cdot b = 1$ *then* $a = b^{-1}$;
(d) *for* $a \neq 0$, $(a^{-1})^{-1} = a$.

<u>proof</u> (0) let us have 1_1 and 1_2, then

$1_1 = 1_1 \cdot 1_2 = 1_2$ so the unit is unique

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

$1 \cdot b = 1 \cdot c \Rightarrow b = c$

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

$1 \cdot b = 1 \Rightarrow b = 1$.

(c) for $a \neq 0$ if $a \cdot b = 1$ then $a = b^{-1}$

multiply by a^{-1} : $(a^{-1} a) b = a^{-1} \cdot 1 = a^{-1}$, so

$b = a^{-1}$. If b^{-1} exists then

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

(d) $(a^{-1})^{-1} \cdot a^{-1} = 1$ multiply by a:

$(a^{-1})^{-1} (a^{-1} a) = a$ or $a = (a^{-1})^{-1}$

Let us now study interrelations between addition and multiplication:

Theorem. 3 (a) $0 \cdot a = 0 \ \forall a \in \mathbb{Q}$.
(b) *if* $a \neq 0$ *and* $b \neq 0$ *then* $ab \neq 0$;
(c) $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$;
(d) $(-a) \cdot (-b) = a \cdot b$.

Proof of (a): $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$, so by Theorem 1(b), $0 \cdot a = 0$, thus proved.

Exercise 3. Complete proofs of (b)-(d):
(b) Assume $a \neq 0$ and $b \neq 0$, but $a \cdot b = 0$. Take the product $0 = a^{-1} \cdot 0 = a^{-1} \cdot (a \cdot b) = \ldots$

$= ((a^{-1}) a) \cdot b = 1 \cdot b = b$, so $b = 0$ - contradiction

Therefore $a \cdot b \neq 0$

(c) $0 = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$, so ...

$(-a) \cdot b = -(a \cdot b)$

same, if $a \cdot (b + (-b)) = a \cdot 0 = 0$ then

$ab + a \cdot (-b) = 0$ and therefore $a \cdot (-b) = -(ab)$

(d) use (c): $(-a) \cdot (-b) = -(a \cdot (-b)) = \ldots$ $-(-(ab)) = ab$

Additional material:

The group is a set G with operation $a \otimes b = c$ defined $\forall a, b \in G$

and such that

(i) $a \otimes (b \otimes c) = (a \otimes b) \otimes c$

(ii) $\exists 1_L$ and 1_R : $\forall a \in G$ $1_L \otimes a = a \otimes 1_R = a$

prove that $1_L = 1_R$: $1_L = 1_L \otimes 1_R = 1_R$

(iii) $\forall a \in G$ $\exists a_L^{-1}$ and a_R^{-1} : $1 = a_L^{-1} \otimes a = a \otimes a_R^{-1}$

prove that $a_L^{-1} = a_R^{-1}$: $a_L^{-1} = a_L^{-1} \otimes (a \otimes a_R^{-1}) = (a_L^{-1} \otimes a) \otimes a_R^{-1} = a_R^{-1}$