Arithmetic topology

Author: Jamal Abo Mokh
Course: 1040158 - Group Theory

Question 1

Define:

$$S(a,b) = a\mathbb{Z} + b$$

such that $a \in \mathbb{N}$

Lemma 1.1

$$a \mid c \implies S(c,b) \subset S(a,b)$$

Proof. assuming $a \mid c$. then we have:

$$a \mid c \implies c = k \cdot a \tag{1.1}$$

let $x \in S(c,b)$, then, there exists m such that:

$$x = c \cdot m + b \overset{(1.1)}{=} (k \cdot a)m + b = a(km) + b$$

Therefore, $x \in S(a,b)$ as required. $\square$

Lemma 1.2 $S(a,b) \cap S(c,b) = S(\mathrm{lcm}(a,c),b)$

Proof. first, since $a, c \mid \mathrm{lcm}(a,c)$, then by lemma (1.1) we have:

$$S(\mathrm{lcm}(a,c),b) \subset S(a,b),\ S(c,b)$$

Therefore, $S(\mathrm{lcm}(a,c),b) \subset S(a,b) \cap S(c,b)$. For the other direction, let $x \in S(a,b) \cap S(c,b)$, therefore, by definition, exists $n, m \in \mathbb{Z}$:

$$x - b = a \cdot m = c \cdot n$$

Since, we have $am = cn$, then by lcm properties we have:

$$\mathrm{lcm}(a,c) \mid am$$

Therefore, $\mathrm{lcm}(a,c) \mid x-b$, hence by lemma (1.1) we have:

$$x \in S(x-b,b) \subset S(\mathrm{lcm}(a,c),b)$$

as required.

$\square$

Corollary 1.1 let $a \in \mathbb{N},\ b,c \in \mathbb{Z}$

$$a \mid c \iff S(c,b) \subset S(a,b)$$

Proof. the $\implies$ direction is proved by lemma (1.1), for the $\impliedby$ direction, we have by the assumption:

$$S(c,b) \subset S(a,b)$$

hence,

$$c+b \in S(c,b) \implies c+b \in S(a,b)$$

therefore,

$$c+b = ma+b \implies a \mid c$$

as required. $\square$

Lemma 1.3 let $a \in \mathbb{N},\ b,c \in \mathbb{Z}$:

$$S(a,b) \cap S(a,c) \neq \emptyset \iff S(a,b) = S(a,c)$$

Proof. let $x \in S(a,b) \cap S(a,c)$, therefore by definition:

$$x = an + b = am + c$$

Consequently,

$$b = a(m-n) + c$$

let $y \in S(a,b)$, therefore:

$$y = an' + b = an' + a(m-n) + c = ak' + c$$

Therefore, $y \in S(a,c)$, the other case is analogs. $\square$

Lemma 1.4 let $a \in \mathbb{N}, b, x \in \mathbb{Z}$, then:

$$x \in S(a,b) \implies S(a,x) = S(a,b)$$

Proof. let $x \in S(a,b)$, since we have $x \in S(a,x)$, then by lemma (1.3), we have:

$$S(a,x) = S(a,b)$$

as required. $\square$

note: this alludes to that this topology acts as ultrametric. since it's saying the set is centerless

Lemma 1.5 let $a \in \mathbb{N},\ b, h \in \mathbb{Z}$, then:

$$S(a,b) \cap S(a,b+h) \neq \emptyset \iff h \bmod a = 0$$

Proof. by lemma (1.3) we have:

$$S(a,b) \cap S(a,b+h) \neq \emptyset \iff S(a,b) = S(a,b+h)$$

hence,

$$S(a,b) \cap S(a,b+h) \neq \emptyset \iff b \in S(a,b+h)$$

Consequently,

$$b = ma + b + h \iff (-m)a = h \iff h \bmod a = 0$$

as required. $\square$

Question 2

Define topology τ on $X = \mathbb{Z}$ by:

$$U \in \tau \iff U = \bigcup \{S(a,b) : (a,b) \in I\}$$

where $I \subset \mathbb{N} \times \mathbb{Z}$

Claim 2.1 τ is topology.

Proof. we'll show

1. it's clear that $\emptyset \in \tau$ by $I = \emptyset$, let $I = \{(1,0)\}$ then $\mathbb{Z} = S(1,0) \in \tau$

2. let $\{V\}$ be a collection of opens sets. take:

$$U = \bigcup V$$

   and let $x \in U$, therefore exists, V_i such that:

$$x \in V_i \implies \exists a, b \in I \;\; x \in S(a,b)$$

   therefore, by (1.4) we have, $S(a,x) = S(a,b)$, hence

$$S(a,x) \subset U$$

   a nghbr of x.

   Hence, we can conclude that, in analogy to open balls, we have, $B(x,r) = S(r,x)$, and the result of the argument follows exactly as regular topology

3. let U, V be open sets. we'll show they are open, and the general result follows by induction.

   let $x \in U \cap V$, therefore, exists $a_1, a_2 \in \mathbb{N}$ such that:

$$x \in S(a_1, x) \subset U, \; x \in S(a_2, x) \in V$$

let $a = \operatorname{lcm}(a_1, a_2)$, therefore, by lemma (1.3) we have:

$$S(a,x) \subset S(a_1,x),\ S(a_2,x)$$

therefore,

$$x \in S(a,x) \subset U \cap V$$

an open nghbr of x as required.

$\square$

Corollary 2.1 if $|A^c| \in \mathbb{N}$ then A is not closed.

Proof. Assume for contradiction that A is closed, then A^c is open by def. since $S(a,b) \subset A^c$, then $|A^c| = \infty$ in contradiction. $\square$

Corollary 2.2 $S(a,b)$ is clopen.

Proof. if $a = 1$, then $S(1,b) = \mathbb{Z}$, hence is trivially clopen. otherwise, assume $a \neq 1$. take the group:

$$G = \mathbb{Z}_a$$

then for any $h \neq 0 \in G$, we have by lemma (1.5):

$$S(a, b+h) \cap S(a,b) = \emptyset$$

since $h \bmod a \neq 0$. let $x \notin S(a,b)$, therefore, we have by (1.3) that:

$$S(a,x) \cap S(a,b) = \emptyset$$

therefore, we take $h = x - b$, hence,

$$S(a, b+h) \cap S(a,b) = \emptyset$$

therefore again by lemma (1.5) we have:

$$(x - b = h) \bmod a \neq 0$$

hence, we have:

$$x \in S(a,x) = S(a,b+h) = S(a,b+[h])$$

since $|G| = a$ is finite, then $S(a,b)^c$ is finite union of open sets, hence, open. therefore,

$$S(a,b)$$

is clopen as required.

$\square$

Question 3

Claim 3.1 there are infinite many prime numbers

Proof. let $\mathbb{P} \subset Z$ be the set of prime numbers.

for any $n \in A = \mathbb{Z} \setminus \{-1, 1\}$, by the theorem of fundamental arithmetic, n can be decomposed into prime numbers or is the 0.

hence, for n, exists $p \in \mathbb{P},\ q \in \mathbb{Z}$ such that:

$$n = pq \implies n \in S(p, 0)$$

with:

$$\forall p \in \mathbb{P} \ \ 0 = p \cdot 0 \in S(p, 0)$$

Therefore,

$$A = \bigcup_{p \in \mathbb{P}} S(p, 0)$$

Now, since $|A^c| = 2 \in \mathbb{N}$, then by corollary (2.1), A cannot be closed.

Assume for contradiction $|\mathbb{P}| \in \mathbb{N}$, then

$$\bigcup_{p \in \mathbb{P}} S(p, 0)$$

is a finite union of closed sets by (2.2), therefore, A is closed, in contradiction $\square$