

# Assignment 1

Naman Mishra

07 January, 2024

**Problem 1.1.** Let  $(\mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, \leq_{\mathbb{Z}})$  be defined as in class. Recall that we identify  $n \in \mathbb{N}$  with  $[(n, 0)] \in \mathbb{Z}$ . Show that any element of  $\mathbb{Z}$  is either  $m$  or  $-m$  for some  $m \in \mathbb{N}$ .

*Proof.* Proved in the last proposition on integers. □

**Problem 1.2.** Recall the construction of  $\mathbb{Q}$  as the set of equivalence classes of the relation  $R$  on  $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$  given by  $(a, b)R(c, d) \iff ad = bc$ . We say that  $[(a, b)] \leq [(c, d)]$  if  $(bc - ad)(bd) \geq 0$ . Using only the arithmetic and order properties of integers, show that the relation  $\leq$  is well-defined. Remember you are not allowed to divide yet!

*Proof.* Proved immediately after the definition. □

**Problem 1.3.** Without assuming the existence of irrational numbers, show that

- (a)  $(\mathbb{Z}, \leq)$  has the least upper bound property.
- (b)  $(\mathbb{Q}, \leq)$  does not have the least upper bound property.

*You may directly cite any theorem(s) proved in class.*

*Proof.*

- (a) Let  $S$  be a non-empty bounded above subset of  $\mathbb{Z}$ . Let  $b$  be an upper bound of  $S$  and let  $f: \mathbb{Z} \rightarrow \mathbb{N}$  be as  $f(x) = b - x$ . By the well-ordering principle,  $f(S)$  has a least element  $m$ . Then  $b - m$  is the maximum of  $S$ .
- (b) Corollary 1.21. □

**Problem 1.4.** Let  $F$  be an ordered field. Recall that  $\mathbb{Q} \subseteq F$ . Show that the following two statements are equivalent.

- (i) For every  $a, b > 0$  in  $F$ , there is an  $n \in \mathbb{N}$  such that  $na > b$ .
- (ii) For every  $a < b$  in  $F$ , there is an  $r \in \mathbb{Q}$  such that  $a < r < b$ .

*Proof.* Suppose (i) holds. Let  $a < b$  in  $F$ . Then  $1/(b - a) > 0$ . Let  $n \in \mathbb{N}$  be such that  $n > 1/(b - a)$ , that is,  $1/n < b - a$ . We first show that there is a rational at most  $a$ . If  $a \geq 0$ , this is trivial. Otherwise,  $-a > 0$  and so by (i) there is an  $m \in \mathbb{N}$  such that  $m > 1/(-a) \iff -1/m < a$ . Thus the set  $S = \{k \in \mathbb{Z} \mid k \cdot \frac{1}{n} \leq a\}$  is non-empty. By (i), it is bounded above. By problem 1.3(a), it has a maximum  $M$ . Then  $\frac{M}{n} \leq a < \frac{M+1}{n} \leq a + \frac{1}{n} < b$ . Thus  $\frac{M+1}{n}$  is the required rational.

Suppose (ii) holds. Let  $0 < a, b$ . Then there exist  $p \in \mathbb{N}$  and  $q \in \mathbb{N}^*$  such that  $0 < b/a < p/q < b/a + 1$ . Since  $1 \leq q$ ,  $p/q \leq p$ . Then  $b < pa$  as required. □

**Problem 1.5.** Let  $F$  be a field. An absolute value of  $F$  is a function  $A: F \rightarrow \mathbb{R}$  satisfying

- (1)  $A(x) \geq 0$  for all  $x \in F$ ,
- (2)  $A(x) = 0$  if and only if  $x = 0$ ,
- (3)  $A(xy) = A(x)A(y)$  for all  $x, y \in F$ ,
- (4)  $A(x + y) \leq A(x) + A(y)$  for all  $x, y \in F$ .

A subset  $S \subseteq F$  is said to be  $A$ -bounded if there exists an  $M > 0$  such that  $A(s) \leq M$  for all  $s \in S$ . This is a way to define boundedness of sets in the absence of an order relation.

Let  $p \in \mathbb{N}$  be a prime number. Define  $\nu_p: \mathbb{Z} \rightarrow \mathbb{Z} \cup \{\infty\}$  by

$$\nu_p(n) = \begin{cases} \max\{k \in \mathbb{N} : p^k \mid n\}, & \text{if } n \neq 0, \\ \infty, & \text{if } n = 0. \end{cases}$$

Extend  $\nu_p$  to  $\mathbb{Q}$  by

$$\nu_p(a/b) = \nu_p(a) - \nu_p(b), \quad a, b \in \mathbb{Z}, b \neq 0.$$

Now, define  $A_p: \mathbb{Q} \rightarrow \mathbb{R}$  by  $A_p(x) = e^{-\nu_p(x)}$  if  $x \neq 0$ , and  $A_p(0) = 0$ .

- (a) Show that  $A_p$  is an absolute value on  $\mathbb{Q}$ .
- (b) Show that

$$A_p(x + y) \leq \max\{A_p(x), A_p(y)\}, \quad x, y \in \mathbb{Q}.$$

- (c) Show that  $\mathbb{Z}$  is  $A_p$ -bounded.

*You may use basic facts about factorization without proof, but clearly state what you are using.*

*Proof.*  $A_p$  satisfies (1) and (2) by definition.

Let  $x = a/b$ ,  $y = c/d$  in  $\mathbb{Q}$ . If either is zero, (3) holds trivially. Otherwise  $xy = ac/bd$  with  $a, b, c, d \in \mathbb{Z}^*$ . Let  $a = p^{\nu_p(a)}a'$ ,  $c = p^{\nu_p(c)}c'$ , where  $a', c'$  are coprime to  $p$ . Then  $ac = p^{\nu_p(a)+\nu_p(c)}(a'c')$ . Thus  $\nu_p(ac) = \nu_p(a) + \nu_p(c)$ . Similarly,  $\nu_p(bd) = \nu_p(b) + \nu_p(d)$ . Thus  $\nu_p(xy) = \nu_p(x) + \nu_p(y)$  and so  $A_p(xy) = A_p(x)A_p(y)$ .

(4) follows from (b), which we prove now. If either  $x$  or  $y$  is zero, (b) holds trivially. Let

$$x = \frac{p^\alpha a}{p^\beta b}, \quad y = \frac{p^\gamma c}{p^\delta d},$$

where  $a, b, c, d \in \mathbb{Z}^*$  are coprime to  $p$ . Thus  $\nu_p(x) = \alpha - \beta$  and  $\nu_p(y) = \gamma - \delta$ . WLOG suppose that  $A_p(x) \geq A_p(y) \iff \nu_p(x) \leq \nu_p(y)$  which gives  $\alpha - \beta \leq \gamma - \delta$ .

$$\begin{aligned} x + y &= \frac{p^{\alpha+\delta}ad + p^{\beta+\gamma}bc}{p^{\beta+\delta}bd} \\ &= \frac{p^{\alpha+\delta}(ad + p^{\beta+\gamma-\alpha-\delta}bc)}{p^{\beta+\delta}bd} \end{aligned}$$

Thus  $\nu_p(x + y) \geq \alpha + \delta - \beta - \delta = \alpha - \beta$  and so  $A_p(x + y) \leq A_p(x) = \max\{A_p(x), A_p(y)\}$ .

(c) follows from  $\nu_p(x) \geq 0$ , so  $A_p(x) \leq 1$  for all  $x \in \mathbb{Z}$ . □