18.100B PROBLEM SET 1

SHUO ZHENG

Problem 1. Let m and n be positive integers with no common factor. Prove that if $\sqrt{m/n}$ is rational, then m and n are perfect squares; that is, there exist integers p and q such that $m = p^2$ and $n = q^2$. (This is proved in Proposition 9 of Book X of *Euclid's Elements*)

Proof. Let $m \in \mathbb{N}$ and $n \in \mathbb{N}$ with no common factor. Suppose $\sqrt{m/n} \in \mathbb{Q}$. Then $\exists! M, N \in \mathbb{N}$ such that M and N have no common factor and

$$\sqrt{\frac{m}{n}} = \frac{M}{N} \implies \frac{m}{n} = \left(\frac{M}{N}\right)^2 = \frac{M^2}{N^2} \implies mN^2 = nM^2;$$

hence, $M^2 | mN^2$ and $N^2 | nM^2$. By the Fundamental Theorem of Arithmetic, there are unique primes $p_1, ..., p_k \in \mathbb{N}$ and exponents $r_1, ..., r_k \in \mathbb{N}$ such that $M = p_1^{r_1} \cdots p_k^{r_k}$. Inductively, assume that $p_1^{2r_1} \cdot \cdot p_k^{2r_k} | m$. Thus,

$$p_{k+1}^{2r_{k+1}} = \frac{M^2}{p_1^{2r_1} \cdots p_k^{2r_k}} \Bigg| \frac{mN^2}{p_1^{2r_1} \cdots p_k^{2r_k}};$$

however, M and N have no common factor, so

$$p_{k+1}^{2r_{k+1}} \Bigg| \frac{m}{p_1^{2r_1} \cdots p_k^{2r_k}} \implies M^2 = p_1^{2r_1} \cdots p_{k+1}^{2r_{k+1}} | m.$$

Similarly, we can obtain $N^2 | n$. Thus, $M^2 | m$ and $N^2 | n$, i.e. $\exists p, q \in \mathbb{N}$ such that $m = pM^2$ and $n = qN^2$; hence,

$$mN^2 = nM^2 \implies pM^2N^2 = qM^2N^2 \implies p = q.$$

Since m and n have no common factor,

$$p = q = 1 \implies m = M^2 \wedge n = N^2.$$

Indeed, m and n are perfect squares. $\square$

Problem 2. Let A and B be two disjoint sets. Suppose further that $|A| = |\mathbb{R}|$ and that $|B| = |\mathbb{N}|$ (i.e. the set B is countable). Show that $|A \cup B| = |\mathbb{R}|$.

Proof. Let A and B be disjoint sets. Suppose $|A| = |\mathbb{R}|$ and $|B| = |\mathbb{N}|$. Then $\exists$ bijective functions $f : A \to \mathbb{R}$ and $g : B \to \mathbb{N}$. Make a function $h : A \cup B \to \mathbb{R}$ such that

$$h(x) = \begin{cases} 2f(x) - 1 & x \in A \wedge f(x) \in \mathbb{N} \\ 2g(x) & x \in B \\ f(x) & x \in A \wedge f(x) \in \mathbb{R} \setminus \mathbb{N} \end{cases}.$$

Date: December 18, 2024.

We want to show that h is bijective ($1-1$ and onto). Assume $h(x) = h(y)$. Since f and g are $1-1$,

$$h(x) \in \{2n-1 : n \in \mathbb{N}\} \implies 2f(x)-1 = 2f(y)-1 \implies f(x) = f(y) \implies x = y$$

and

$$h(x) \in \{2n : n \in \mathbb{N}\} \implies 2g(x) = 2g(y) \implies g(x) = g(y) \implies x = y$$

and

$$h(x) \in \mathbb{R} \setminus \mathbb{N} \implies f(x) = f(y) \implies x = y.$$

Thus, $x = y$. Assume $z \in \mathbb{R}$. Since f and g are onto,

$$z \in \{2n-1 : n \in \mathbb{N}\} \implies \exists x \in A, f(x) = \frac{z+1}{2} \in \mathbb{N} \implies h(x) = 2f(x) - 1 = z$$

and

$$z \in \{2n : n \in \mathbb{N}\} \implies \exists x \in B, g(x) = \frac{z}{2} \in \mathbb{N} \implies h(x) = 2g(x) = z$$

and

$$z \in \mathbb{R} \setminus \mathbb{N} \implies \exists x \in A, f(x) = z \in \mathbb{R} \setminus \mathbb{N} \implies h(x) = f(x) = z.$$

Thus, $\exists x \in A \cup B$ with $h(x) = z$. Indeed, $|A \cup B| = |\mathbb{R}|$. □

Problem 3. Fix $b > 1$.

(a) If m, n, p, q are integers, $n > 0$, $q > 0$, and $r = m/n = p/q$, prove that

$$(b^m)^{\frac{1}{n}} = (b^p)^{\frac{1}{q}}.$$

Hence it makes sense to define $b^r := (b^m)^{\frac{1}{n}}$. (How could it have failed to make sense?)

Proof. Let $m, n, p, q \in \mathbb{Z}$ with $n > 0$ and $q > 0$. If $r = m/n = p/q$, then $mq = pn$; hence,

$$[(b^m)^{\frac{1}{n}}]^{nq} = (b^m)^q = b^{mq} = b^{pn} = (b^p)^n = [(b^p)^{\frac{1}{q}}]^{nq}.$$

Given Theorem 1.21, $\exists! x \in \mathbb{R}$ such that

$$b^{mq} = x^{nq} = b^{pn} \implies (b^m)^{\frac{1}{n}} = x = (b^p)^{\frac{1}{q}}.$$

Thus, $(b^m)^{\frac{1}{n}} = (b^p)^{\frac{1}{q}}$, i.e. defining

$$b^r := (b^m)^{\frac{1}{n}}$$

makes sense; else, b^r cannot be well-defined. □

(b) Prove that $b^{r+s} = b^r b^s$ if r, s are rational.

Proof. Let $r \in \mathbb{Q}$ and $s \in \mathbb{Q}$. Then $\exists m, n, p, q \in \mathbb{Z}$ where $n > 0$ and $q > 0$ such that

$$r = \frac{m}{n} \wedge s = \frac{p}{q} \implies r + s = \frac{m}{n} + \frac{p}{q} = \frac{mq + pn}{nq}.$$

Given Theorem and Corollary 1.21,

$$(b^r b^s)^{nq} = b^{mq} b^{pn} = b^{mq+pn};$$

hence,

$$b^r b^s = (b^{mq+pn})^{\frac{1}{nq}} = b^{r+s}.$$

□

(c) If x is real, define $B(x)$ to be the set of all numbers b^t, where t is rational and $t \leq x$. Prove that

$$b^r = \sup B(r)$$

when r is rational. Hence it makes sense to *define*

$$b^x := \sup B(x)$$

for every real x.

Proof. Let $x \in \mathbb{R}$. Define the set

$$B(x) := \{b^t \in \mathbb{R} : t \in \mathbb{Q} \text{ and } t \leq x\}.$$

Choose $r, q \in \mathbb{Q}$. If $r \geq q$, then $\exists m, n \in \mathbb{Z}$ such that $n > 0$ and

$$\frac{m}{n} = r - q \geq 0.$$

Given that $b > 1$, $b^m \geq 1$; however,

$$0 < (b^m)^{\frac{1}{n}} = b^{r-q} < 1 \implies 0 < b^m < 1,$$

a contradiction, i.e. $b^{r-q} \geq 1$. Hence, $b^r = b^{r-q}b^q \geq b^q$, i.e. b^r is an upper bound of $B(r)$. Note that $b^r \in B(r)$. Thus, $b^r = \sup B(r)$, i.e. defining

$$b^x := \sup B(x)$$

makes sense. $\square$

(d) Prove that $b^{x+y} = b^x b^y$ for all real x and y.

Proof. Let $x \in \mathbb{R}$ and $y \in \mathbb{R}$. Choose $r, s \in \mathbb{Q}$. If $r \leq x$ and $s \leq y$, then $r + s \leq x + y$; hence,

$$b^r b^s = b^{r+s} \leq b^{x+y}.$$

Thus,

$$b^r \leq \frac{b^{x+y}}{b^s} \implies b^x \leq \frac{b^{x+y}}{b^s};$$

else, $b^x \neq \sup B(x)$. Similarly, we have that

$$b^s \leq \frac{b^{x+y}}{b^x} \implies b^y \leq \frac{b^{x+y}}{b^x};$$

otherwise, $b^y \neq \sup B(y)$. Thus, $b^x b^y \leq b^{x+y}$; hence, either $b^x b^y < b^{x+y}$ or $b^x b^y = b^{x+y}$. Suppose, for obtaining a contradiction, that $b^x b^y < b^{x+y}$. Thus, $\exists t \in \mathbb{Q}$ such that $t < x + y$ and

$$b^x b^y < b^t < b^{x+y};$$

otherwise, $b^{x+y} \neq \sup B(x + y)$. By Theorem 1.20($a$), $\exists N \in \mathbb{N}$ such that

$$N(x + y - t) > 1;$$

hence,

$$t < x + y - \frac{1}{N}.$$

Given Theorem 1.20(b), $\exists r, s \in \mathbb{Q}$ such that

$$x - \frac{1}{2N} \leq r \leq x \wedge y - \frac{1}{2N} \leq s \leq y;$$

hence,

$$x + y - \frac{1}{N} \leq r + s \leq x + y.$$

Thus, $b^t < b^{r+s} = b^r b^s \leq b^x b^y$, which is a contradiction. Indeed, $b^x b^y = b^{x+y}$. □

Problem 4. Prove that no order can be defined in the complex field that turns it into an ordered field. (*Hint:* -1 is a square.)

Proof. Suppose, for obtaining a contradiction, an order $<$ can be defined in $\mathbb{C}$ making it into an ordered field. By Proposition 1.18,

$$-1 = i^2 \geq 0 \implies 0 \leq 1 = 1 + 0 \leq 1 + (-1) = 0$$

hence,

$$0 = 1,$$

a contradiction. □

Problem 5. Prove that

$$|x+y|^2 + |x-y|^2 = 2|x|^2 + 2|y|^2$$

if $x, y \in \mathbb{R}^n$. Interpret this geometrically, as a statement about parallelograms.

Proof. Let $x \in \mathbb{R}^n$ and $y \in \mathbb{R}^n$. Then $\exists x_1, ..., x_n, y_1, ..., y_n \in \mathbb{R}$,

$$x = (x_1, ..., x_n) \wedge y = (y_1, ..., y_n);$$

hence,

$$\begin{aligned} |x+y|^2 + |x-y|^2 &= \sum_{i=1}^{n} (x_i + y_i)^2 + \sum_{i=1}^{n} (x_i - y_i)^2 \\ &= \sum_{i=1}^{n} (x_i^2 + 2x_i y_i + y_i^2) + \sum_{i=1}^{n} (x_i^2 - 2x_i y_i + y_i^2) \\ &= \sum_{i=1}^{n} (2x_i^2 + 2y_i^2) \\ &= 2\sum_{i=1}^{n} x_i^2 + 2\sum_{i=1}^{n} y_i^2 = 2|x|^2 + 2|y|^2. \end{aligned}$$

Geometrically, we interpret vectors x and y as forming a parallelogram; hence, the sum of the diagonal length squared $|x+y|^2$ and anti-diagonal length squared $|x-y|^2$ is the sum of the side lengths squared $2|x|^2$ and $2|y|^2$. □

Problem 6. Suppose $f : \mathbb{R} \to \mathbb{R}$ is a function such that for all real numbers x and y the following two equations hold

$$f(x+y) = f(x) + f(y), \tag{1}$$

$$f(xy) = f(x)f(y). \tag{2}$$

Claim: $f(x) = 0$ for all x or $f(x) = x$ for all x.
Prove this claim using the following steps:

(a) Prove that $f(0) = 0$ and that $f(1) = 0$ or 1.
(b) Prove that $f(n) = nf(1)$ for every integer n and then that $f(n/m) = (n/m)f(1)$ for all integers n, m such that $m \neq 0$. Conclude that either $f(q) = 0$ for all rational numbers q or $f(q) = q$ for all rational numbers q.
(c) Prove that f is increasing, that is to say that $f(x) \geq f(y)$ whenever $x \geq y$ for any real numbers x and y.

(d) Prove that if $f(1) = 0$ then $f(x) = 0$ for all real numbers x. Prove that if $f(1) = 1$ then $f(x) = x$ for all real numbers x.

Proof. Let $x \in \mathbb{R}$ and $y \in \mathbb{R}$.

(a) If $x = y = 0$, then

$$f(x) + f(y) = f(x+y) \implies f(0) + f(0) = f(0) \implies f(0) = 0.$$

If $x = y = 1$, then

$$\begin{aligned} f(xy) = f(x)f(y) \implies f(1) = f(1)^2 &\implies f(1)(1 - f(1)) = 0 \\ &\implies f(1) = 0 \vee 1. \end{aligned}$$

If $x = y$, then

$$f(xy) = f(x)f(y) \implies f(x^2) = f(x)^2.$$

If $x + y = 0$, then $y = -x$ and

$$\begin{aligned} f(x) + f(y) = f(x+y) &\implies f(x) + f(-x) = f(0) = 0 \\ &\implies f(-x) = -f(x). \end{aligned}$$

(b) Suppose, for induction, that

$$\forall k \in \mathbb{Z}, f(k) = kf(1).$$

Then

$$f(k+1) = f(k) + f(1) = kf(1) + f(1) = (k+1)f(1),$$

and

$$f(k-1) = f(k) + f(-1) = kf(1) - f(1) = (k-1)f(1);$$

hence,

$$\forall n \in \mathbb{Z}, f(n) = nf(1).$$

Thus,

$$\begin{aligned} m \in \mathbb{Z} \setminus \{0\} &\implies f(n) = f\left(\frac{n}{m}\right) f(m) \\ &\implies nf(1) = f\left(\frac{n}{m}\right) mf(1) \\ &\implies \frac{n}{m} f(1) = f\left(\frac{n}{m}\right) f(1) = f\left(\frac{n}{m}\right) \\ &\implies f\left(\frac{n}{m}\right) = \frac{n}{m} f(1); \end{aligned}$$

hence, $f(q) = 0$ for all $q \in \mathbb{Q}$ or $f(q) = q$ for all $q \in \mathbb{Q}$.

(c) If $x \geq y$, then $x - y \geq 0$; hence, $\exists t \in \mathbb{R}$ such that $x - y = t^2$ (Theorem 1.21). Thus,

$$f(x) - f(y) = f(x-y) = f(t^2) = f(t)^2 \geq 0 \implies f(x) \geq f(y);$$

hence, f is increasing.

(d) Given $n \in \mathbb{N}$, $\exists p, q \in \mathbb{Q}$ such that

$$x - \frac{1}{n} \leq p \leq x \leq q \leq x + \frac{1}{n}$$

(Theorem 1.20(b)). If $f(1) = 0$, then

$$0 = f(p) \leq f(x) \leq f(q) = 0 \implies f(x) = 0$$

(because f is increasing). If $f(1) = 1$, then

$$x - \frac{1}{n} \leq p = f(p) \leq f(x) \leq f(q) = q \leq x + \frac{1}{n} \implies f(x) = x$$

(because n is arbitrary).

Thus, $f(x) = 0$ or $f(x) = x$ and $f(y) = 0$ or $f(y) = y$, as desired. $\square$