Problem Set 1, 18.100B/C, Fall 2011

Michael Andrews
Department of Mathematics
MIT

September 21, 2011

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 both perfect squares, that is to say 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 Euclids Elements).

Assume $\sqrt{m/n}$ is rational. Then there exist positive integers M and N with no common factor such that $\sqrt{m/n} = M/N$ and so $mN^2 = nM^2$.

Claim: M^2 divides m and N^2 divides n.

Assume the claim for now. Then

$$m = M^2m' \text{ and } n = N^2n' \text{ for some } m' \text{ and } n'.$$

Substituting we obtain $M^2m'N^2 = N^2n'M^2$ which gives $m' = n'$. $m' = n'$ divides m and n so $m' = n' = 1$ and we have shown m and n are perfect squares.

Proof of claim: We show that M^2 divides m; the argument that N^2 divides n is identical. Write M as a product of primes $p_1 \cdots p_r$ and note that no p_i divides N. Assume inductively that $p_1^2 \cdots p_t^2$ divides m. Then

$$p_{t+1}^2 \,\Big|\, \frac{M^2}{p_1^2 \cdots p_t^2} \,\Big|\, \frac{m}{p_1^2 \cdots p_t^2} N^2$$

Since p_{t+1} does not divide N^2 we see

$$p_{t+1}^2 \,\Big|\, \frac{m}{p_1^2 \cdots p_t^2}, \text{ which gives } p_1^2 \cdots p_{t+1}^2 \,\Big|\, m.$$

The inductive hypothesis holds when $t = 0$; the empty product is 1. Thus, by induction $p_1^2 \cdots p_r^2 = M^2$ divides m.

2

Problem 6 from page 22.

Fix $b > 1$

a

$$\frac{m}{n} = \frac{p}{q} \implies mq = pn$$

so that

$$((b^m)^{1/n})^{nq} = (b^m)^q = b^{mq} = b^{pn} = (b^p)^n = ((b^p)^{1/q})^{nq}.$$

By uniqueness of nq^{th} roots

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

b

Let $r, s \in \mathbb{Q}$. Write $r = m/n$ and $s = p/q$ where $m, p \in \mathbb{Z}$ and $n, q \in \mathbb{N}$. Since nq is an integer we know that

$$(b^r b^s)^{nq} = (b^r)^{nq}(b^s)^{nq}$$

but

$$(b^r)^{nq} = ((b^m)^{1/n})^{nq} = (b^m)^q = b^{mq}$$

and similarly $(b^s)^{nq} = b^{np}$. Since mq and np are integers we can conclude

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

Since there is a unique positive real number y such that $y^{nq} = b^{mq+np}$, we obtain

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

c

For $x \in \mathbb{R}$ let

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

Suppose we are given $r \in \mathbb{Q}$. If $y \in B(r)$ then we can write $y = b^t$, where $t \in \mathbb{Q}$ and $t \leq r$. Since $t, r \in \mathbb{Q}$ we immediately obtain

$$y = b^t \leq b^r$$

which shows b^r is an upper bound for $B(r)$. Since $b^r \in B(r)$ it is clear that it is the least upper bound and we conclude

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

Perhaps one needs to check that for $t, r \in \mathbb{Q}$ with $t \leq r$ one does actually have $b^t \leq b^r$. By (b) it suffices to show that for $s \in \mathbb{Q}$ with $s \geq 0$ we have $b^s \geq 1$. Writing $s = m/n$ for $m \in \mathbb{N} \cup \{0\}$, $n \in \mathbb{N}$, we have $b^m \geq 1$, since $b > 1$; by the contapositive of the statement "$0 \leq b^{m/n} < 1$ implies $b^m = (b^{m/n})^n < 1$," we are done.

The point regarding the deduction is as follows. Given $x \in \mathbb{R}$ the set $B(x)$ is bounded above and so $\sup B(x)$ is a number, which exists for all $x \in \mathbb{R}$ and we propose setting $b^x = \sup B(x)$. However, we already have a definition for b^r when r is rational; we have just checked that our new definiton does not clash with our old one.

d

Let $x, y \in \mathbb{R}$. Suppose $r, s \in \mathbb{Q}$, $r \leq x$ and $s \leq y$. Then

$$r + s \leq x + y \implies b^{r+s} \in B(x+y) \implies b^{r+s} \leq b^{x+y}.$$

Thus

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

Since this holds for all $r \in \mathbb{Q}$ with $r \leq x$, $\frac{b^{x+y}}{b^s}$ is an upper bound for $B(x)$. Thus

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

Since this holds for all $s \in \mathbb{Q}$ with $s \leq y$ we have

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

Suppose for contradiction that $b^x b^y < b^{x+y}$. Then $b^x b^y$ is not an upper bound for $B(x+y)$ and there exists a $t \in \mathbb{Q}$ with $t \leq x + y$ and $b^x b^y < b^t$. By the argument of 3(e) we can assume that $t < x + y$. (This is valid because t is rational and so we do not use what we are supposed to be proving!)

Choose $r, s \in \mathbb{Q}$ with $r \leq x$, $s \leq y$ and $t \leq r + s \leq x + y$ (we'll show how to do this below). Since $r \leq x$ and $s \leq y$ we have $b^r \leq b^x$ and $b^s \leq b^y$, which gives $b^r b^s \leq b^x b^y$. Thus

$$b^x b^y < b^t \leq b^{r+s} = b^r b^s \leq b^x b^y,$$

a contradiction, and we have proved $b^x b^y = b^{x+y}$.

To choose r and s as above proceed as follows. Choose $N \in \mathbb{N}$ such that $N(x + y - t) \geq 1$ and pick $r, s \in \mathbb{Q}$ such that $x - \frac{1}{2N} \leq r \leq x$ and $y - \frac{1}{2N} \leq s \leq y$. (Notice that we could have imposed strict inequalities everywhere.)

3

Problem 7 from page 22.

Fix $b > 1, y > 0$ and let n be a positive integer.

a

$$b^n - 1 = (b^{n-1} + b^{n-2} + \ldots + b + 1)(b-1) \geq n(b-1).$$

b

Replacing b with $b^{1/n}$ we obtain

$$b - 1 \geq n(b^{1/n} - 1).$$

This is permissable since $b > 1$ implies $b^{1/n} > 1$.

c

Let $t > 1$ and $n > (b-1)/(t-1)$. Then

$$n(t-1) > b - 1 \geq n(b^{1/n} - 1).$$

Thus $t > b^{1/n}$.

d

Let w be a real number such that $b^w < y$. Then $t = yb^{-w} > 1$. Choose $n \in \mathbb{N}$ such that $n > (b-1)/(t-1)$. Then

$$b^{1/n} < t = yb^{-w} \implies b^{w+1/n} < w.$$

e

Let w be a real number such that $b^w > y$. Then $t = b^w/y > 1$. Choose $n \in \mathbb{N}$ such that $n > (b-1)/(t-1)$. Then

$$b^{1/n} < t = b^w/y \implies y < b^{w-1/n}.$$

f

Let $A = \{w : b^w < y\}$ and let $x = \sup A$.

Suppose that $b^x < y$. By *d*) we can choose n so that $b^{x+1/n} < y$. Then $x + 1/n \in A$ and x is not an upper bound for A, a contradiction.

Suppose that $b^x > y$. By *e*) we can choose n so that $b^{x-1/n} > y$. Given $w \in A$

$$b^w < y < b^{x-1/n}.$$

Thus $w < x - 1/n$. This means $x - 1/n$ is an upper bound for A, meaning that x is not the least upper bound, a contradiction.

Thus $b^x = y$.

This all sounds good but really we need to prove that $b^w < b^{x-1/n}$ does indeed give $w < x - 1/n$. First we show that if $a \in \mathbb{R}$ and $b^a > 1$ then $a > 0$. Well, by definition of b^a in 6) there exists an integer $m \in \mathbb{Z}$ and positive integer $n \in \mathbb{N}$ such that $m/n \leq a$ and $b^{m/n} > 1$; 1 is not an upper bound for the set of numbers b^t, where t is rational and $t \leq a$. Then $b^m = (b^{m/n})^n > 1$, which gives $m > 0$. Thus $a \geq m/n > 0$. Now $b^w < b^{x-1/n}$ implies $b^{x-1/n-w} > 1$, which gives $x - 1/n - w > 0$ so $x - 1/n > w$ as we claimed.

g

Suppose $x' > x$. Then $x' - x > 0$. We can find a rational $q \in \mathbb{Q}$ such that $x' - x > q > 0$. Then $b^{x-x'} \geq b^q$ by definition and $b^q > 1$. Thus $b^{x-x'} > 1$ and $b^x > b^{x'}$. In particular, if $x \neq x'$ then $b^x \neq b^{x'}$, so the x constructed above must be unique.

4

Prove that no order can be defined in the complex field that turns it into an ordered field.

Suppose that such an order exists. We know that in any ordered field squares are greater than or equal to zero. Since $i^2 = -1$, this means that $0 \leq -1$. Thus

$$1 = 0 + 1 \leq -1 + 1 = 0 \leq 1,$$

which implies $0 = 1$, a contradiction.

5

Let $\mathbb{R}$ be the set of real numbers and suppose $f : \mathbb{R} \longrightarrow \mathbb{R}$ 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.

a

Setting $x = 1$ and $y = 0$ in equation (1) gives

$$f(1) = f(1) + f(0) \text{ so that } f(0) = 0.$$

Setting $x = y = 1$ in equation (2) gives $f(1) = f(1)^2$. Thus $f(1)$ is equal to 0 or 1 as we may see by solving the equation $x - x^2 = x(1 - x) = 0$.

Remark: If I did not have to answer all parts of the question fully and I just wanted to prove the claim as quickly as possible I would proceed by noting that $f(1) = 0$ gives

$$f(x) = f(1)f(x) = 0 \text{ for all } x \in \mathbb{R}.$$

From this moment on I could then assume $f(1) = 1$.

b

By a) we have

$$f(0) = 0 = 0f(1).$$

Also,

$$f(x) + f(-x) = f(x - x) = f(0) = 0 \text{ so that } f(-x) = -f(x) \text{ for all } x \in \mathbb{R}.$$

In particular, $f(-1) = -f(1)$.

Let $n \in \mathbb{Z}$ and assume that $f(n) = nf(1)$. Then

$$f(n+1) = f(n) + f(1) = nf(1) + f(1) = (n+1)f(1)$$

and

$$f(n-1) = f(n) + f(-1) = nf(1) - f(1) = (n-1)f(1).$$

By induction $f(n) = nf(1)$ for all $n \in \mathbb{Z}$.

For $n, m \in \mathbb{Z}$, $m \neq 0$

$$f\left(\frac{n}{m}\right) mf(1) = f\left(\frac{n}{m}\right) f(m) = f(n) = nf(1)$$

and so

$$f\left(\frac{n}{m}\right) = f\left(\frac{n}{m}\right) f(1) = \frac{n}{m} f(1).$$

Thus $f(q) = qf(1)$ for all $q \in \mathbb{Q}$ and by a) either $f(q) = 0$ for all $q \in \mathbb{Q}$ or $f(q) = q$ for all $q \in \mathbb{Q}$.

c

Suppose $x \geq 0$. Then there exists a $y \in \mathbb{R}$ such that $y^2 = x$ and

$$f(x) = f(y^2) = f(y)^2 \geq 0.$$

Thus

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

d

Suppose $f(1) = 0$. Given any $x \in \mathbb{R}$ we can find $p, q \in \mathbb{Q}$ such that

$$p \leq x \leq q.$$

Then

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

Alternatively, we proceed as remarked in a).

Suppose $f(1) = 1$. Let $x \in \mathbb{R}$ and $n \in \mathbb{N}$. Then there exist $p, q \in \mathbb{Q}$ such that

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

and so

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

So for all $x \in \mathbb{R}$ and all $n \in \mathbb{N}$ we have

$$x - \frac{1}{n} \leq f(x) \leq x + \frac{1}{n}$$

which gives $f(x) = x$ for all $x \in \mathbb{R}$.