MATH 112: HOMEWORK 2 SOLUTIONS

JOHANN GAEBLER

Rudin: Problem 6

We will use the following lemmas throughout problems 6 and 7.

Lemma 1.1. *If $1 < b \in \mathbb{R}$, $r \in (-\infty, 0)$, $r \in \mathbb{Q}$, then $b^r < 1$. Likewise, if $r \in (0, \infty)$, $r \in \mathbb{Q}$, then $b^r > 1$.*

Proof. First suppose r is positive. Write r as $\frac{p}{q}$. Then, by Problem 6, part 1 (which we will prove without this lemma below), $b^r = (b^p)^{1/q}$. By the field axioms, $\beta = b^p > 1$. Then, either $\beta^{1/p} < 1$ or > 1 (do you see why it can't $= 1$?); if $\beta^{1/p} < 1$, then, by the field axioms and Theorem 1.21, $(\beta^{1/p})^p = \beta < 1$, which is a contradiction. Therefore $b^r = \beta^{1/p} > 1$.

Lemma 1.2. *If $m, n \in \mathbb{N}$, $1 < b \in \mathbb{R}$, then $b^{1/n} = (b^m)^{1/mn}$.*

Proof. Note that since m, n are integers, by the field axioms, $(b^{1/n})^{mn} = ((b^{1/n})^n)^m = b^m = ((b^m)^{1/mn})^{mn}$. Therefore, since both $b^{1/n}$, $(b^m)^{1/mn}$ are mn-th roots of b^m, by the uniqueness part of Theorem 1.21, they are equal □

However, if r is negative, $-r = r \cdot -1$ is positive, so by the preceding, $0 < b < b^{-r}$. Thus, by Proposition 1.18 and Problem 6, part 2, $0 < b^r < b^{-1} < 1$. □

(a): We need to show that b^r is well-defined. Since one rational number can be represented by many different fractions, we need to show that for equivalent representations of the same rational number, we get the same answer. Namely, we need to show that if $\frac{p}{q} = \frac{m}{n}$, $(b^p)^{1/q} = (b^m)^{1/n}$. We know by Theorem 1.21 that

$$\left((b^p)^{1/q}\right)^{qn} = \left(\left(b^p\right)^{1/q}\right)^q\Big)^n = b^{pn} = b^{mq} = \left(\left(b^m\right)^{1/n}\right)^q\Big)^{qn} = \left(b^m\right)^{1/n}\Big)^{qn}$$

Therefore $(b^p)^{1/q}$ and $(b^m)^{1/n}$ are nq-th roots of b^{pn}, and since, by Theorem 1.21, this root is unique possibly up to sign, they are equal, because by the lemma they are both positive.

(b): We use the same trick (namely, showing that they both are n-th roots of the same number). Using lemma 2,

$$\left((b^{pn+mq})^{1/nq}\right)^{nq} = b^{pn+mq} = (b^{pn})(b^{mq}) = \left(((b^{pn})(b^{mq}))^{1/nq}\right)^{nq}$$
$$= \left((b^{pn})^{1/nq}(b^{mq})^{1/nq}\right)^{nq} = \left((b^p)^{1/q}(b^m)^{1/n}\right)^{nq}$$

Therefore $(b^{pn+mq})^{1/nq}$ and $(b^p)^{1/q}(b^m)^{1/n}$ are both nq-th roots of b^{pn+mq}; therefore they are equal.

(c): Suppose $\beta \in B(r)$; then $\exists t \in (0, r]$ s.t. $\beta = b^t$. However, by part 2, $b^r/b^t = b^{r-t} < 1$ by lemma 1, so $b^r > b^t = \beta$. Therefore, b^r is an upper-bound; since $b^r \in B(r)$, it is necessarily the supremum. (Do you see why an upper bound that is actually in the set in question must be the supremum?)

(d): We need to show that $\sup(B(x+y)) = \sup(B(x))\sup(B(y))$. However, if $s \leq x$, $t \leq y$, $s+t \leq x+y$, we get that $B(x) \cdot B(y) \subset B(x+y)$.[1] Moreover, if $z \in \mathbb{Q}$, $z \leq x+y$, then there exist rational s', t' such that $z - y \leq s' \leq x$ and $z - x \leq t' \leq y$. Therefore $z < s' + t'$, and $b^{s'+t'} \in B(x)B(y)$, we get that $b^z < b^{s'+t'}$, whence $\sup(B(x+y)) \leq \sup(B(x)B(y))$ (do you see why?).

Thus, if we can show that $\sup(B(x)B(y)) = \sup(B(x))\sup(B(y))$, then we are done. However, it follows by definition that $\sup(B(x)B(y)) \leq \sup(B(x))\sup(B(y))$. Moreover, suppose $\sup(B(x)B(y)) < \sup(B(x))\sup(B(y))$; then choose $s \leq x$ and $t \leq y$ such that

$$\frac{\sup(B(x)B(y))}{b^x} < b^s \leq b^x = \frac{B(x) \quad \sup(B(x)B(y))}{b^y} < b^t \leq b^y = B(y)$$

Then $\sup(B(x)B(y)) < b^{s+t} \in B(x)B(y)$, which is absurd. Therefore $\sup(B(x)B(y)) = \sup(B(x))\sup(B(y))$, i.e., $b^{x+y} = b^x b^y$. □

Rudin: Problem 7

(a): By the binomial theorem, for $c \geq 0$,

$$(c+1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k c^{n-k} = b^n + \sum_{k=1}^{n-2} \binom{n}{k} c^{n-k} + nc + 1 = c^n + \sum_{k=1}^{n} 1 \geq c^n + nc + 1$$

Since by the field axioms $c^k > 0$ for all k. Setting $b - 1 = c$ gives the desired result.

(b): By lemma 1, $b^{1/n} > 1$; therefore, the inequality from part 1 gives $(b^{1/n})^n - 1 = b - 1 \geq n(b^{1/n} - 1)$.

(c): We derive the inequality

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

Rearranging gives $t - 1 > b^{1/n} - 1$, as desired.

(d): Using the Archimedean property, choose $n > \frac{b-1}{yb^{-w}-1}$; then $b^{1/n} > yb^{-w} \implies b^{w+1/n} > y$.

(e): Using the Archimedean property, choose $n > \frac{b-1}{b^w y^{-1}}$; then $b^{1/n} > y^{-1}b^w \implies b^{w-1/n} > y$.

(f): Suppose $b^x < y$; then, by part (d), there exists n such that $b^{x+1/n} < y$; therefore $x + 1/n \in A$, which is impossible since $x = \sup(A)$.

Now suppose $b^x > y$; then, by part (e), there exists n such that $b^{x-1/n} > y$; therefore $x - 1/n$ is an upper bound for A, which is impossible since x is the supremum.

Therefore $b^x = y$.

(g): To show that x is unique, suppose $b^{x'} = y$; then if $x' > x$, $1 = b^{x-x'} < 1$ by lemma 1;if $x > x'$, $1 = b^{x'-x} < 1$. Since both of these are impossible, $x = x'$. Therefore x is unique. □

Problem 3

Note that if $[a] = [b]$ and $[c] = [d]$, then there exist $n_1, n_2 \in \mathbb{Z}$ such that $a = n_1 p + b$, $c = n_2 p + d$. Therefore, $a + c = (n_1 + n_2)p + c + d$ and $ac = (n_1 n_2 p + n_1 d + n_2 b)p + cd$. Therefore if $a \sim b$ and $c \sim d$, then $a + c \sim b + d$ and $ac \sim bd$.

Now, to show all of the field axioms (except the existence of a multiplicative inverse), note that because all (except the existence of a multiplicative inverse) hold for $\mathbb{Z}$, we can derive that:

(1) $[a] + [b] = [a + b]$ and $[a + b]$ is an equivalence class.
(2) $[a] + [b] = [a + b] = [b + a] = [b] + [a]$.
(3) $([a] + [b]) + [c] = ([a + b]) + [c] = [a + b] + [c] = [a + b + c] = [a] + [b + c] = [a] + ([b] + [c])$.
(4) $[a] + [0] = [a + 0] = [a]$.
(5) $[a] + [-a] = [a - a] = [0]$.
(6) $[a][b] = [ab]$ and $[ab]$ is an equivalence class.

[1] When we write AB for A, B sets, we mean the set $\{x \in \mathbb{R} : \exists a \in A, b \in B \text{ s.t. } x = ab\}$.

(7) $[a][b] = [ab] = [ba] = [b][a]$
(8) $([a][b])[c] = [ab][c] = [abc] = [a][bc] = [a]([b][c])$
(9) $[a][1] = [a1] = [a]$
(10) $[a]([b] + [c]) = [a][b + c] = [a(b + c)] = [ab + ac] = [ab] + [ac]$

Now, to address the existence of a multiplicative inverse, note that because p is prime, $ab \neq p$ for $0 < a, b < p$. We wish to show that $ab \neq np$ for all $n \in \mathbb{Z}$. To this end, recall Bezout's Identity, which states that there exist $m, n' \in \mathbb{Z}$ such that $1 = mp + n'b$. Multiplying through by a gives that $a = amp + an'b = amp + n'np = p(am + nn')$, which is impossible since $|a| < |p|$ and $|am + nn'| = 0$ or is greater than 1.

Therefore, for any $c \sim a$, $d \sim b$, then $cd \sim ab \not\sim p$, i.e., $[c][d] \neq [0]$ for $c, d \not\sim p$.

Now, it is clear that if $0 < a, b < p$, then there does not exist $n \in \mathbb{Z}$ such that $a = np + b$, since $|a - b| < |p| \leq |np|$. Therefore, the equivalence classes $[0], [1], \ldots, [p - 1]$ are all distinct; moreover, by the Euclidean algorithm, for all $n \in \mathbb{Z}$ such that $n < 0$ or $n \geq p$, we immediately see that $n \sim a$ for some $0 \leq a < p$. Thus, there are precisely p equivalence classes.

Now, I claim that if $[a] \neq [0]$ and $[b] \neq [c]$, then $[ab] \neq [ac]$; this follows by rearragement: $[a][b - c] \neq 0$ by the foregoing, so $[ab] \neq [ac]$.

Thus $[a0], [a1], \ldots, [a(p - 1)]$ are all distinct equivalence classes, and there are p of them; thus, again by the foregoing, at least one of them must be [1]; let it be $[ab]$. Then, we see immediately that $[b] = [a]^{-1}$. □

Problem 4

Suppose we could order $\mathbb{Z}/p\mathbb{Z}$. Then either $[0] < [1]$ or $[0] > [1]$. In either case, by the axioms for ordered fields, we get that $[0] > [1] + \cdots + [1] = \sum_{k=1}^{p} [1] = [p][1] = [p] = [0]$ or $[0] < [1] + \cdots + [1] = \sum_{k=1}^{p} [1] = [p][1] = [p] = [0]$, i.e., $[0] > [0]$, which is contradictory. Therefore there is no ordering on $\mathbb{Z}/p\mathbb{Z}$. □