Math 207 First Midterm Solutions

December 12, 2006

1. (a) Let $d \in \mathbb{Z}$ such that $d > 1$ and define a relation on $\mathbb{Z}$ by $a \sim b$ if there exists $k \in \mathbb{Z}$ such that $a - b = kd$. Show that $\sim$ is an equivalence relation, that addition and multiplication are well defined on equivalence classes, and that the set of equivalence classes forms a commutative ring with 1. We shall denote this ring as $\mathbb{Z}/(d)$.

   Proof. First, we must show that $\sim$ is an equivalence relation.

   i. *(Reflexive)* $\forall a \in \mathbb{Z}$, $a - a = 0 = 0 * d$ so $a \sim a$.
   ii. *(Symmetric)* If $a \sim b$, then $a - b = kd \Rightarrow b - a = (-k)d$.
   iii. *(Transitive)* If $a \sim b$ and $b \sim c$ then $a - b = k_1 d$ and $b - c = k_2 d$ so $a - c = (a - b) + (b - c) = k_1 d + k_2 d = (k_1 + k_2)d$.

   Next, we show that $+$ and $*$ are well defined. Let $a \sim a', b \sim b'$. Then $\exists k_1, k_2 \in \mathbb{Z}$ such that $a = a' + k_1 d, b = b' + k_2 d$. Thus we have

$$\begin{aligned}(a+b) - (a'+b') &= ((a' + k_1 d) + (b' + k_2 d)) - (a' + b') \\ &= (k_1 + k_2)d\end{aligned}$$

   and so $(a + b) \sim (a' + b')$. Similarly,

$$\begin{aligned}ab - a'b' &= ((a' + k_1 d) * (b' + k_2 d)) - (a'b') \\ &= (a'b' + a'k_2 d + k_1 db + k_1 k_2 d^2) - a'b' \\ &= (a'k_2 + k_1 b + k_1 k_2 d)d\end{aligned}$$

   so $ab \sim a'b'$. Thus multiplication is well defined. Let us denote the class of a by $[a]$ We have shown $[a]+[b] = [a+b]$ and $[a][b] = [ab]$. We inherit the properties of a ring from the corresponding properties of $\mathbb{Z}$. For example, $[-a] + [a] = [-a + a] = [0]$, $[1][a] = [1 * a] = [a]$, and $[a]([b] + [c]) = [a][b + c] = [a(b + c)] = [ab + ac] = [a][b] + [a][c]$. □

   (b) For what values of d is $\mathbb{Z}/(d)$ an integral domain?

   Proof. $\mathbb{Z}/(d)$ is an integral domain if and only if d is a prime. If d is composite, then $d = ab$ with $1 < a, b < d$, $a, b \in \mathbb{Z}$, and so $[a][b] = [d] = [0] = [0][b]$ but $[a] \neq 0$ and $[b] \neq 0$. Conversely, if d is prime and $[a][b] = [a][c]$, then $[a(b-c)] = [0]$, so $a(b-c) = dk$ for some $k \in \mathbb{Z}$ Since d is prime, one of a and $(b-c)$ must be a multiple of d, and hence either $[a] = 0$ or $[b] = [c]$. □

(c) Show that $\mathbb{Z}/(d)$ can never be made into an ordered integral domain.

Proof. Assume that we could find some ordering $<$ for $\mathbb{Z}/(d)$. As proved in class, $[0] < [1]$. Therefore, $[n] < [n+1]$ for all $n \in \mathbb{Z}$. In particular, $[0] < [1] < \ldots < [d-1] < [d]$, hence by transitivity, $[0] < [d] = [0]$. This violates trichotomy, so no such ordering can exist. □

2. Show that any finite integral domain is a field.

Proof. Let R be a finite integral domain with elements $\{a_1, \ldots, a_n\}$. If $a_i \neq 0$, consider the set $a_iR = \{a_ia_1, a_ia_2, \ldots a_ia_n\} = \{a_ir \mid r \in R\}$. All n elements of this set are distinct elements of R because if $a_ib = a_ic$, then $b = c$, so $a_iR = R$. In particular, $1 \in a_iR$, so for some $r \in R$, $a_ir = ra_i = 1$. Thus, each a_i has a multiplicative inverse, and R is a field. □

3. (a) Let $(a_i)_{i\in\mathbb{N}}$ and $(b_i)_{i\in\mathbb{N}}$ be Cauchy sequences with $a_i, b_i \in \mathbb{Q}$. Define $c_i = a_ib_i$. Prove that $(c_i)_{i\in\mathbb{N}}$ is a Cauchy sequence.

Proof. First, we need a lemma.

Lemma 1. *Every Cauchy sequence is bounded.*

Proof. Let (a_i) be a Cauchy sequence. Then there exists $N \in \mathbb{N}$ such that for all $m, n > N$, $|a_m - a_n| < 1$. By the triangle inequality, $|a_i| \leq \max(|a_1|, \ldots |a_N|, |a_{N+1}| + 1)\ \forall i \in \mathbb{N}$. □

Let M be a bound for both (a_i) and (b_i), so that $|a_i| < M$ and $|b_i| < M$ for all $i \in \mathbb{N}$. Let $\epsilon > 0$. Then there exist $N_1, N_2 \in \mathbb{N}$ such that $|a_m - a_n| < \epsilon/2M$ for all $m, n > N_1$ and $|b_m - b_n| < \epsilon/2M$ for all $m, n > N_2$. Let $N > \max(N_1, N_2)$. If $m, n > N$, then

$$\begin{aligned}
|a_mb_m - a_nb_n| &= |a_mb_m - a_mb_n + a_mb_n - a_nb_n| \\
&= |a_m(b_m - b_n) + b_n(a_m - a_n)| \\
&\leq |a_m(b_m - b_n)| + |b_n(a_m - a_n)| \\
&= |a_m|\,|b_m - b_n| + |b_n|\,|a_m - a_n| \\
&< M(\epsilon/2M) + M(\epsilon/2M) = \epsilon.
\end{aligned}$$

Thus, (a_ib_i) is a Cauchy sequence. □

(b) Let $(a_i)_{i\in\mathbb{N}}$ and $(b_i)_{i\in\mathbb{N}}$ be sequences with $a_i, b_i \in \mathbb{Q}$, $b_i \neq 0$. Suppose that there exist $a, b \in \mathbb{Q}$, $b \neq 0$ such that (a_i) converges to a and (b_i) converges to b. Define $c_i = \frac{a_i}{b_i}$. Prove that (c_i) converges to $\frac{a}{b}$.

Proof. A similar calculation to the one in the previous solution shows that

$$\left|\frac{a_i}{b_i} - \frac{a}{b}\right| \leq \frac{|a_i - a|\,|b| + |a|\,|b - b_i|}{|b_i|\,|b|}.$$

Let $\epsilon > 0$. Let $N_1 \in \mathbb{N}$ such that $|b - b_n| < |b|/2$ for all $n > N_1$, let $N_2 \in \mathbb{N}$ such that $|a - a_n| < \epsilon\,|b|/4$, and if $|a| \neq 0$, let $N_3 \in \mathbb{N}$ such that $|b - b_n| < \epsilon(|b|^2 / |a|)/4$ for all $n > N_3$. Let $N > \max(N_1, N_2, N_3)$. Note that if $n > N_1$, then $|b_n| > |b|/2$. Then for all $n > N$, we have that

$$\begin{aligned}
\left|\frac{a_n}{b_n} - \frac{a}{b}\right| &\leq \frac{|a_n - a|\,|b| + |a|\,|b - b_n|}{|b_n|\,|b|} \\
&< \frac{(\epsilon\,|b|/4)\,|b| + |a|\,\epsilon(|b|^2 / |a|)/4}{|b|^2/2} \\
&= 2(\epsilon/4 + \epsilon/4) = \epsilon.
\end{aligned}$$

Thus, (c_i) converges to a/b. □

4. Let $K = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Show that K is an ordered subfield of $\mathbb{R}$ in which the least upper bound property does not hold.

Proof. Let $a, b, c, d \in \mathbb{Q}$. Then $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in K$ and $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in K$ so K is closed under addition and multiplication. Since $K \subset \mathbb{R}$, addition and multiplication are associative, commutative, and distributive. Since $0, 1 \in \mathbb{Q}$, we have that $0, 1 \in K$. If $a, b \in \mathbb{Q}$, then $-a, -b \in \mathbb{Q}$, and since $(a + b\sqrt{2}) + (-a + -b\sqrt{2}) = 0$, K has additive inverses. Thus K is a commutative ring with 1. If $a, b \in \mathbb{Q}$ are not both zero, then since $\sqrt{2}$ is irrational, $\frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in \mathbb{Q}$, and since $(a+b\sqrt{2})(\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}) = 1$, K has multiplicative inverses. Thus K is a field.

Since K is a field and a subset of $\mathbb{R}$, K is a subfield of $\mathbb{R}$, and since $\mathbb{R}$ is ordered, we can restrict the ordering to K to turn K into an ordered subfield. If a subset $A \subset K$ has a least upper bound, then since K is dense in $\mathbb{R}$, A has the same least upper bound when viewed as a subset of $\mathbb{R}$. Thus, if we let $A = \{x \in K \mid x < \pi\}$, then $\sup(A) = \pi \notin K$, and thus K does not satisfy the least upper bound property.

□