Math 3210 § 2. **First Midterm Exam** Name: Solutions
Treibergs January 30, 2019

1. *Prove that for every natural number n the quantity $n^3 - n$ is divisible by 6.*

   We argue by induction.

   Base Case. When $n = 1$, $n^3 - n = 1^3 - 1 = 0 = 6 \cdot 0$ which is divisible by six.

   Induction Case. We assume for some $n \in \mathbb{N}$ that $n^3 - n$ is divisible by 6, which means that there is $k \in \mathbb{Z}$ so that $n^3 - n = 6k$. The $n + 1$ term is

   $$(n+1)^3 - (n+1) = n^3 + 3n^2 + 2n + 1 - (n+1) = n^3 - n + 3n^2 + 3n.$$

   By the induction hypothesis,

   $$(n+1)^3 - (n+1) = 6k + 3n(n+1).$$

   Now either n or $n + 1$ is even so that $n(n+1)$ is divisible by two. Thus $n(n+1) = 2j$ for some $j \in \mathbb{Z}$, hence

   $$(n+1)^3 - (n+1) = 6k + 3 \cdot 2j = 6(k+j),$$

   which is divisible by six.

   Since the base case holds and the induction hypothesis implies that the $(n+1)^3 - (n+1)$ is also divisible by six, by induction we conclude $n^3 - n$ is divisible by 6 for all $n \in \mathbb{N}$.

2. *Recall the axioms of a field $(\mathcal{F}, +, \times)$. For any $x, y, z \in \mathcal{F}$,*

[A1.]	*(Commutativity of Addition)*	$x + y = y + x$.
[A2.]	*(Associativity of Addition)*	$x + (y + z) = (x + y) + z$.
[A3.]	*(Additive Identity)*	$(\exists\, 0 \in \mathcal{F})\, (\forall\, t \in \mathcal{F})\ 0 + t = t$.
[A4.]	*(Additive Inverse)*	$(\exists\, {-x} \in \mathcal{F})\ x + (-x) = 0$.
[M1.]	*(Commutativity of Multiplication)*	$xy = yx$.
[M2.]	*(Associativity of Multiplication)*	$x(yz) = (xy)z$.
[M3.]	*(Multiplicative Identity)*	$(\exists\, 1 \in \mathcal{F})\ 1 \neq 0$ *and* $(\forall\, t \in \mathcal{F})\ 1t = t$.
[M4.]	*(Multiplicative Inverse)*	*If* $x \neq 0$ *then* $(\exists\, x^{-1} \in \mathcal{F})\ (x^{-1})x = 1$.
[D.]	*(Distributivity)*	$x(y + z) = xy + xz$.

   Using only the field axioms, show that for any $a, b \in \mathcal{F}$ such that $b \neq 0$, then

   $$a + (b^{-1}) = (ab + 1)(b^{-1})$$

   Justify every step of your argument using just the axioms listed here.

   [Hint: the first line of your argument must not be "$a + (b^{-1}) = (ab + 1)(b^{-1})$."]

   Starting from the left side, we deduce a sequence of equalities that are justified by the axioms and end up with the right side.

$a + (b^{-1})$	Start at the left hand side.
$= 1a + 1(b^{-1})$	Multiplicative identity. (M3)
$= 1a + (b^{-1})1$	Commutivity of multiplication. (M1)
$= ((b^{-1})b)a + (b^{-1})1$	Multiplicative inverse: since $b \neq 0$ there is a b^{-1} such that $(b^{-1})b = 1$. (M4)
$= (b^{-1})(ba) + (b^{-1})1$	Associativity of multiplication. (M2)
$= (b^{-1})((ba) + 1)$	Distributive. (D)
$= ((ba) + 1)(b^{-1})$	Commutivity of multiplication. (M1)
$= ((ab) + 1)(b^{-1})$	Commutivity of multiplication. (M1)

Thus all expressions are equal to each other and also to the right side of the equation, proving the asserted equation.

3. *Determine whether the following statements are true or false. If true, give a proof. If false, give a counterexample.*

   (a) *If $f : A \to B$ then $f(f^{-1}(E)) = E$ for every subset $E \subset B$.*
   FALSE. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = x^2$ and $E = [-4, 4]$. Then $f^{-1}(E) = [-2, 2]$ and $f(f^{-1}(E)) = [0, 4]$, which is not the same as E.

   (b) *Let $f : A \to B$ and $g : B \to C$ be functions. If both f and g are onto then the composite function $g \circ f : A \to C$ defined by $g \circ f(x) = g(f(x))$ is onto.*
   TRUE. To show that $g \circ f$ is onto, we show that for any choice of $z \in C$ there is an $x \in A$ such that $g \circ f(x) = z$. Since g is onto there is $y \in B$ so that $g(y) = z$. Since f is onto there is $x \in A$ so that $f(x) = y$. The same also works for the composite: $g \circ f(x) = g(f(x)) = g(y) = z$, hence $g \circ f$ satisfies the condition to be onto.

   (c) *Let U denote the universal set and A, B be any subsets of U. Then their complements satisfy $(A \backslash B)^c = A^c \backslash B^c$.*
   FALSE. Let $U = \mathbb{R}$, $A = (-\infty, 1]$ and $B = [0, \infty)$. Then $A \backslash B = (-\infty, 0)$. Also $A^c = (1, \infty)$ and $B^c = (-\infty, 0)$ so that $A^c \backslash B^c = (1, \infty)$ which is not the same as $(A \backslash B)^c = [0, \infty)$.

4. *Recall that the rational numbers are defined to be the set of equivalence classes $\mathbb{Q} = S/\sim$ where $S = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0 \right\}$ is the set of symbols (pairs of integers) and the symbols are equivalent if they represent the same fraction $\frac{a}{b} \sim \frac{c}{d}$ iff $ad = bc$. We denote the equivalence class, the "fraction," $\left[\frac{a}{b}\right]$ to distinguish it from a symbol from S. Addition and multiplication of rationals, for example, is defined on equivalence classes by*

$$\left[\frac{m}{n}\right] + \left[\frac{r}{t}\right] = \left[\frac{mt + nr}{nt}\right], \qquad \left[\frac{m}{n}\right] \cdot \left[\frac{r}{t}\right] = \left[\frac{mr}{nt}\right].$$

   (a) *Show that multiplication of rationals is well defined: it does not depend on the choice of the symbols representing the fractions.*
   We have to show that if we choose different representatives of the equivalence classes then we get equivalent products. Taking

$$\frac{m'}{n'} \sim \frac{m}{n} \quad \text{so } m'n = mn' \text{ and} \qquad \frac{p'}{q'} \sim \frac{p}{q} \quad \text{so } p'q = pq'$$

   we have

$$\frac{m'p'}{n'q'} \sim \frac{mp}{nq}$$

because

$$(m'p')(nq) = m'np'q = mn'pq' = (mp)(n'q').$$

Define the subset $\mathcal{P} = \left\{ x \in \mathbb{Q} : \text{there are } p \geq 0 \text{ and } q > 0 \text{ such that } x = \left[\frac{p}{q}\right] \right\}$. $\mathcal{P}$ *may be regarded as nonnegative rational numbers from which an order may be defined for* $x, y \in \mathbb{Q}$ *by* $x \geq y$ *if and only if* $x - y \in \mathcal{P}$. *Order properties follow from properties of* $\mathcal{P}$:

(b) *Show that if* $x, y \in \mathcal{P}$ *then* $x + y \in \mathcal{P}$. *Show that therefore, the order defined on the rationals is transitive: for* $x, y, z \in \mathbb{Q}$ *if* $x \leq y$ *and* $y \leq z$ *then* $x \leq z$.

Let

$$x = \left[\frac{m}{n}\right] \in \mathcal{P} \quad \text{and} \quad y = \left[\frac{p}{q}\right] \in \mathcal{P}.$$

Being in $\mathcal{P}$ means that $\dfrac{m}{n} \sim \dfrac{m'}{n'}$ and $\dfrac{p}{q} \sim \dfrac{p'}{q'}$ such that $m', p' \geq 0$ and $n', q' > 0$. But then,

$$x + y = \left[\frac{m'}{n'}\right] + \left[\frac{p'}{q'}\right] = \left[\frac{m'q' + n'p'}{n'q'}\right] \in \mathcal{P}.$$

This is because $n' > 0$ and $q' > 0$ imply $n'q' > 0$ and since also $m' \geq 0$ and $p' \geq 0$, the four inequalities imply $m'q' + n'p' \geq 0$.

Now suppose $x, y, z \in \mathbb{Q}$ such that $x \leq y$ and $y \leq z$. By the definition of $x \leq y$ in $\mathbb{Q}$ we have $y - x \in \mathcal{P}$. By the definition of $y \leq z$ in $\mathbb{Q}$ we have $z - y \in \mathcal{P}$. By what was proved above, the sum of two rationals in $\mathcal{P}$ is in $\mathcal{P}$ so $(y - x) + (z - y) \in \mathcal{P}$. But this equals $(y - x) + (z - y) = z - x \in \mathcal{P}$. Hence $x \leq z$ by definition of $x \leq z$ in $\mathbb{Q}$.

5. *Let* $E \subset \mathbb{R}$ *be a set of real numbers given by*

$$E = \{x \in \mathbb{R} : \quad (\forall t > 0) \quad (\exists s < t) \quad x \leq s \quad \}.$$

Find E *and and prove your result.*

Writing the set as union and intersection we find

$$E = \bigcap_{t>0} \bigcup_{s<t} (-\infty, s] = \bigcap_{t>0} (-\infty, t) = (-\infty, 0].$$

To prove it, if $x \in E$ then $(\forall t > 0) \quad (\exists s < t) \quad x \leq s$. But real numbers such that $(\exists s < t)$ $x \leq s$ satisfy $x < t$. So $(\forall t > 0)$ $x < t$ implies $x \leq 0$. Hence $x \in (-\infty, 0]$.

On the other hand, if $x \in (-\infty, 0]$ then $x \leq 0$. But then, $(\forall t > 0)$ $x \leq 0 < t$. For such a t, let $s = 0$ which satisfies $x \leq s < t$. It follows that $(\forall t > 0)(\exists s < t)$ $x \leq s$, which is the condition to be in E.