University of Toronto – MAT246H1-S – LEC0201/9201

Concepts in Abstract Mathematics

Final Exam

Jean-Baptiste Campesato

April 16th, 2021 at 2pm to April 17th, 2021 at 2pm

Write your solutions concisely but without skipping important steps.
You can rely on all the material covered in the course (lecture notes, slides, weekly questions and problem sets).
You can use results from other questions of the exam by quoting them properly, even if you did not solve them.
Each question should be submitted in a separate picture on Crowdmark. Make sure that your submission is legible.

Exercise 1. 15 P.

Prove that $\forall n \in \mathbb{N} \setminus \{0,1\},\ 2^n - 1 > n$.

Exercise 2. 20 P.

1. Prove that $\forall m \in \mathbb{N} \setminus \{0\},\ \forall x \in \mathbb{R},\ x^m - 1 = (x-1)\left(\sum_{k=0}^{m-1} x^k\right)$.
2. Let $n \in \mathbb{N} \setminus \{0\}$. Prove that if n is a composite number then $2^n - 1$ is composite too.
   Recall that a natural number n is composite if and only if there exist $a, b \in \mathbb{N} \setminus \{0,1\}$ such that $n = ab$.
3. We say that $n \in \mathbb{N} \setminus \{0,1\}$ is 2-prime if $2^n \equiv 2 \pmod{n}$.
   Prove that if n is 2-prime then $2^n - 1$ is 2-prime too.
4. Deduce that there are infinitely many composite 2-prime numbers.
   We admit that 341 is 2-prime.

Exercise 3. 15 P.

Let p be a prime number. Prove that $\forall a, b \in \mathbb{Z},\ a^p \equiv b^p \pmod{p} \implies a^p \equiv b^p \pmod{p^2}$.

Exercise 4. 15 P.

We set $D \coloneqq \left\{ \frac{m}{2^n} \ :\ m \in \mathbb{Z},\ n \in \mathbb{N} \right\}$.
Prove that D is dense in $\mathbb{R}$, i.e. prove that $\forall x, y \in \mathbb{R},\ x < y \implies \exists d \in D,\ x < d < y$.

Exercise 5. 20 P.

Define $\theta : \mathbb{Z} \times \mathbb{Z} \to \mathbb{R}$ by $\theta(a,b) = a + b\sqrt{2}$.

1. Is θ surjective?
2. Prove that θ is injective.
3. We set $\mathbb{Z}\left[\sqrt{2}\right] \coloneqq \left\{ a + b\sqrt{2} \ :\ a, b \in \mathbb{Z} \right\}$. Prove that $\left|\mathbb{Z}\left[\sqrt{2}\right]\right| = \aleph_0$.

Exercise 6. 15 P.

1. Prove that $\left|\mathbb{R}^{\mathbb{Q}}\right| = |\mathbb{R}|$ where $\mathbb{R}^{\mathbb{Q}}$ is the set of functions $\mathbb{Q} \to \mathbb{R}$.
2. We denote by $C^0(\mathbb{R})$ the set of continuous functions $\mathbb{R} \to \mathbb{R}$.
   Prove that $\Phi : \begin{cases} C^0(\mathbb{R}) & \to & \mathbb{R}^{\mathbb{Q}} \\ f & \mapsto & f_{|\mathbb{Q}} \end{cases}$ is injective, where $f_{|\mathbb{Q}}$ denotes the restriction of f to $\mathbb{Q}$.
   Remark: recall from your calculus course that if $f \in C^0(\mathbb{R})$ and $\lim\limits_{n\to+\infty} x_n = \ell$ then $\lim\limits_{n\to+\infty} f(x_n) = f(\ell)$.
   Hint: don't forget you can use results from problem sets.
3. Prove that $\left|C^0(\mathbb{R})\right| = |\mathbb{R}|$.

Sample solutions to Exercise 1.
Let's prove the statement by induction on $n \geq 2$.

- *Base case at $n = 2$:* $2^n - 1 = 2^2 - 1 = 3 > 2 = n$.
- *Induction step.* Assume that $2^n - 1 > n$ holds for some $n \geq 2$. Then

$$\begin{aligned} 2^{n+1} - 1 = 2 \times 2^n - 1 &= 2(2^n - 1) + 1 \\ &> 2n + 1 \quad \text{by the induction hypothesis} \\ &> n + 1 \quad \text{since } n > 0 \end{aligned}$$

  Which ends the induction step.

Comment: I asked this question to evaluate your writings for proof by inductions (since I insisted a lot on it this term) and I picked this statement to prove by induction because it is useful for Exercises 2 and 4.

Sample solutions to Exercise 2.

1. *Comment: Several students complained by e-mail that there is an issue when $x = 0$ because 0^0 is undefined, but you use the convention $0^0 = 1$ all the time for such formulae, e.g.:*
   - *Binomial formula:* $\forall x, y \in \mathbb{R}, \forall n \in \mathbb{N}, (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$
   - *Geometric sum:* $\forall x \in \mathbb{R} \setminus \{1\}, \forall n \in \mathbb{N}, \sum_{k=0}^{n} x^k = \frac{1-x^{n+1}}{1-x}$
   - *When defining a polynomial function* $f : \mathbb{R} \to \mathbb{R}$ *by* $f(x) = \sum_{k=0}^{n} a_k x^k$
   - *When we proved that for finite sets* $\left|E^F\right| = |E|^{|F|}$ *(including the case* $E = F = \varnothing$*)*
   - ...

   Method 1:
   Let $x \in \mathbb{R}$.
   We are going to prove that $\forall m \in \mathbb{N} \setminus \{0\}$, $x^m - 1 = (x-1)\left(\sum_{k=0}^{m-1} x^k\right)$ by induction on $m \geq 1$.

   - *Base case at $m = 1$:* $(x-1)\left(\sum_{k=0}^{1-1} x^k\right) = (x-1)x^0 = x - 1 = x^1 - 1$.
   - *Induction step.* Assume that $x^m - 1 = (x-1)\left(\sum_{k=0}^{m-1} x^k\right)$ for some $m \geq 1$. Then

$$\begin{aligned} (x-1)\left(\sum_{k=0}^{m} x^k\right) = (x-1)\left(\sum_{k=0}^{m-1} x^k + x^m\right) &= (x-1)\sum_{k=0}^{m-1} x^k + (x-1)x^m \\ &= (x^m - 1) + (x-1)x^m \quad \text{by induction hypothesis} \\ &= x^m - 1 + x^{m+1} - x^m = x^{m+1} - 1 \end{aligned}$$

     which ends the induction step.

   Method 2:
   Let $m \in \mathbb{N} \setminus \{0\}$ and $x \in \mathbb{R}$. Then we have the following telescoping sum:

$$(x-1)\left(\sum_{k=0}^{m-1} x^k\right) = x\left(\sum_{k=0}^{m-1} x^k\right) - \sum_{k=0}^{m-1} x^k = \sum_{k=0}^{m-1} x^{k+1} - \sum_{k=0}^{m-1} x^k = \sum_{k=1}^{m} x^k - \sum_{k=0}^{m-1} x^k = x^m - x^0 = x^m - 1$$

2. Let n be a composite number. Then $n = ab$ for some $a, b \in \mathbb{N} \setminus \{0, 1\}$.
   Therefore
   $$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)\left(\sum_{k=0}^{b-1} 2^{ak}\right) \quad \text{by Question 1 since } b \in \mathbb{N} \setminus \{0\}$$
   Since $a > 1$, by Exercise 1, $2^a - 1 > a > 1$.
   Besides $\sum_{k=0}^{b-1} 2^{ak} \geq 2^0 + 2^a > 1$ since $b > 1$.
   Therefore $2^n - 1$ is composite.

3. **Method 1:**
   Let $n \in \mathbb{N} \setminus \{0, 1\}$ be a 2-prime number. Then $2^n \equiv 2 \pmod{n}$, so that $2^n = 2 + \lambda n$ for some $\lambda \in \mathbb{Z}$.
   Note that, by Exercise 1 as $n \in \mathbb{N} \setminus \{0, 1\}$, $2^n - 1 > n \geq 2$. Thus $2^n - 1 \in \mathbb{N} \setminus \{0, 1\}$ and $\lambda > 0$.
   Therefore
   $$2^{2^n-1} - 2 = 2^{2+\lambda n-1} - 2 = 2^{1+\lambda n} - 2 = 2\left(2^{\lambda n} - 1\right) = 2\left(\left(2^n\right)^\lambda - 1\right)\right) = 2\left(2^n - 1\right)\left(\sum_{k=0}^{\lambda-1} 2^{nk}\right) \quad \text{by Q1 since } \lambda > 0.$$
   So $2^n - 1 | 2^{2^n-1} - 2$, i.e. $2^{2^n-1} \equiv 2 \pmod{2^n - 1}$.
   Hence $2^n - 1$ is 2-prime.

   Method 2:
   Let $n \in \mathbb{N} \setminus \{0, 1\}$ be a 2-prime number. Then $2^n \equiv 2 \pmod{n}$, so that $2^n = 2 + \lambda n$ for some $\lambda \in \mathbb{Z}$.
   Note that, by Exercise 1 as $n \in \mathbb{N} \setminus \{0, 1\}$, $2^n - 1 > n \geq 2$. Thus $2^n - 1 \in \mathbb{N} \setminus \{0, 1\}$ and $\lambda > 0$.
   Therefore $2^{2^n-1} = 2^{2+\lambda n-1} = 2^{1+\lambda n} = 2 \times (2^n)^\lambda \equiv 2 \times 1^\lambda \pmod{2^n - 1} \equiv 2 \pmod{2^n - 1}$.
   Hence $2^n - 1$ is 2-prime.

4. Assume by contradiction that the set of composite 2-prime numbers is finite, then it is bounded.
   Besides it is non-empty since $341 = 11 \times 31$ is a composite 2-prime number.
   Therefore there exists a greatest composite 2-prime number N (*Chapter 2, Theorem 17*).
   By Questions 2 and 3, $2^N - 1$ is a composite 2-prime number too since $N \geq 341 > 1$.
   Besides $2^N - 1 > N$ by Exercise 1 since $N \geq 341 > 1$.
   Hence a contradiction since N is the greatest composite 2-prime number.

Sample solutions to Exercise 3.
Let $a, b \in \mathbb{Z}$ be such that $a^p \equiv b^p \pmod{p}$.
By Fermat's little theorem, since p is prime, we know that $a^p \equiv a \pmod{p}$ and that $b^p \equiv b \pmod{p}$.
Therefore $a \equiv b \pmod{p}$. Thus there exists $\lambda \in \mathbb{Z}$ such that $a = b + \lambda p$.
Then $a^p = (b+\lambda p)^p = \sum_{k=0}^{p} \binom{p}{k} b^{p-k} (\lambda p)^k = b^p + pb^{p-1}\lambda p + \sum_{k=2}^{p} \binom{p}{k} b^{p-k} \lambda^k p^k \equiv b^p + 0 + \sum_{k=2}^{p} 0 \pmod{p^2} \equiv b^p \pmod{p^2}$
(note that $p^2 | pb^{p-1}\lambda p = p^2 b^{p-1}\lambda$ and that $p^2 | p^k$ for $k \geq 2$).

Sample solutions to Exercise 4.
We adapt the proof of Theorem 45 from Chapter 6, using 2^n as denominator instead of n.
Let $x, y \in \mathbb{R}$ be such that $x < y$.
Set $\varepsilon = y - x > 0$.
By the archimedean property of $\mathbb{R}$, there exists $n \in \mathbb{N}$ such that $n\varepsilon > 1$.
Note that $n > 0$, since otherwise $0 > 1$. Therefore $\frac{1}{n} < \varepsilon$.
Note that $2^n > n$. Indeed if $n > 1$ then $2^n > n + 1 > n$ by Exercise 1, otherwise if $n = 1$ then $2^1 = 2 > 1$.
Thus $0 < \frac{1}{2^n} < \frac{1}{n} < \varepsilon$.
Set $m = \lfloor 2^n x \rfloor + 1$, then $2^n x < m \leq 2^n x + 1$, so $x < \frac{m}{2^n} \leq x + \frac{1}{2^n} < x + \varepsilon = y$.
Hence $d = \frac{m}{2^n} \in D$ satisfies $x < d < y$.

Sample solutions to Exercise 5.

1. **Method 1:**
We are going to prove that $\sqrt{3} \notin \mathrm{Im}(\theta)$.
Assume by contradiction that there exists $(a, b) \in \mathbb{Z}^2$ such that $\theta(a, b) = \sqrt{3}$. Then $\sqrt{3} = a + b\sqrt{2}$.
   - If $a = 0$, then $\sqrt{3} = b\sqrt{2}$, so that $3 = 2b^2$ with $b^2 \in \mathbb{Z}$. Then $2|3$ which is impossible.
   (*alternatively: if $a = 0$ then $\frac{3}{2} = b^2 \in \mathbb{Z}$, which is impossible*).
   Hence $a \neq 0$.
   - If $b = 0$, then $\sqrt{3} = a \in \mathbb{Q}$. Which is impossible.
   Hence $b \neq 0$.

   Squaring $\sqrt{3} = a + b\sqrt{2}$, we get $3 = a^2 + 2b^2 + 2ab\sqrt{2}$, so that $\sqrt{2} = \frac{3-a^2-2b^2}{2ab} \in \mathbb{Q}$.
   Which is a contradiction. Hence $\sqrt{3} \notin \mathrm{Im}(\theta)$ and θ is not surjective.

   Method 2:
   We are going to prove that $\sqrt{3} \notin \mathrm{Im}(\theta)$.
   Assume by contradiction that there exists $(a, b) \in \mathbb{Z}^2$ such that $\theta(a, b) = \sqrt{3}$.
   Then $\sqrt{3} = a + b\sqrt{2}$, so that $\sqrt{3} - b\sqrt{2} = a$.
   Squaring the previous equality, we get $3 + 2b^2 - 2b\sqrt{6} = a^2$.
   Note that $b \neq 0$ since otherwise $\sqrt{3} = a \in \mathbb{Q}$ which is impossible.
   Therefore $\sqrt{6} = \frac{3+2b^2-a^2}{2b} \in \mathbb{Q}$ which is a contradiction. Hence $\sqrt{3} \notin \mathrm{Im}(\theta)$ and θ is not surjective.

   Method 3:
   We are going to prove that $\frac{314}{42} \notin \mathrm{Im}(\theta)$ (or anything in $\mathbb{Q} \setminus \mathbb{Z}$).
   Assume by contradiction that there exists $(a, b) \in \mathbb{Z}^2$ such that $\theta(a, b) = \frac{314}{42}$. Then $\frac{314}{42} = a + b\sqrt{2}$.
   - First case: if $b = 0$ then $\frac{314}{42} = a \in \mathbb{Z}$. Hence a contradiction.
   - Second case: if $b \neq 0$ then $b\sqrt{2} \notin \mathbb{Q}$ by Week 9, Ex 4.4, since $\sqrt{2} \notin \mathbb{Q}$ and $b \in \mathbb{Q} \setminus \{0\}$.
   But $b\sqrt{2} = \frac{314}{42} - a \in \mathbb{Q}$. Hence a contradiction.

   Therefore $\frac{314}{42} \notin \mathrm{Im}(\theta)$ and θ is not surjective.

   Method 4: We are going to prove that $\frac{1}{2} \notin \mathrm{Im}(\theta)$.
   Assume by contradiction that there exists $(a, b) \in \mathbb{Z}^2$ such that $\theta(a, b) = \frac{1}{2}$.
   Then $\frac{1}{2} = a + b\sqrt{2} \implies b\sqrt{2} = \frac{1}{2} - a \implies 2b^2 = \frac{1}{4} + a^2 - a \implies \frac{1}{4} = 2b^2 - a^2 + a \in \mathbb{Z}$.
   Hence a contradiction.
   Therefore $\frac{1}{2} \notin \mathrm{Im}(\theta)$ and θ is not surjective.

   Method 5: We are going to prove that $\frac{\sqrt{2}}{2} \notin \mathrm{Im}(\theta)$.
   Assume by contradiction that there exists $(a, b) \in \mathbb{Z}^2$ such that $\theta(a, b) = \frac{\sqrt{2}}{2}$.
   Then $\frac{\sqrt{2}}{2} = a + b\sqrt{2}$, so that $\left(\frac{1}{2} - b\right)\sqrt{2} = a$. Note that $\frac{1}{2} \notin \mathbb{Z}$ so that $b \neq \frac{1}{2}$, hence $\sqrt{2} = \frac{a}{1/2-b} \in \mathbb{Q}$.
   Hence a contradiction. Therefore $\frac{\sqrt{2}}{2} \notin \mathrm{Im}(\theta)$ and θ is not surjective.

   Method 6: Since $|\mathbb{N}| = |\mathbb{Z}|$, we have $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}| = \aleph_0 < |\mathbb{R}|$.
   Therefore, there is no surjection $\mathbb{Z} \times \mathbb{Z} \to \mathbb{R}$, so that θ can't be surjective.

2. Let $(a,b),(c,d) \in \mathbb{Z}^2$ be such that $\theta(a,b) = \theta(c,d)$.
   Then $a + b\sqrt{2} = c + d\sqrt{2}$, i.e. $(a-c) + (b-d)\sqrt{2} = 0$.
   - If $b \neq d$, then $\sqrt{2} = \frac{c-a}{b-d} \in \mathbb{Q}$, which is impossible.
   - If $b = d$, then $a - c = 0$, so that $(a,b) = (c,d)$.

   Therefore θ is injective.

3. **Method 1:**
   Note that $\mathrm{Im}(\theta) = \mathbb{Z}\left[\sqrt{2}\right]$ by definition of $\mathbb{Z}\left[\sqrt{2}\right]$.
   Therefore $\tilde{\theta} : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\left[\sqrt{2}\right]$ defined by $\tilde{\theta}(a,b) = \theta(a,b)$ is well-defined and surjective.
   Besides, it is injective (and hence bijective) by the previous question.
   Hence $\left|\mathbb{Z}\left[\sqrt{2}\right]\right| = |\mathbb{Z}\times\mathbb{Z}| = |\mathbb{N}\times\mathbb{N}| = \aleph_0$ since $|\mathbb{Z}| = |\mathbb{N}|$.

   Method 2:
   Since $|\mathbb{Z}| = |\mathbb{N}|$, we get $|\mathbb{Z}^2| = |\mathbb{Z}\times\mathbb{Z}| = |\mathbb{N}\times\mathbb{N}| = \aleph_0$.
   So $\mathbb{Z}\left[\sqrt{2}\right] = \bigcup_{(a,b)\in\mathbb{Z}^2} \left\{a + b\sqrt{2}\right\}$ is countable as a countable union of countable sets (singletons).
   Thus $\left|\mathbb{Z}\left[\sqrt{2}\right]\right| \leq \aleph_0$.
   Besides $\mathbb{Z} \subset \mathbb{Z}\left[\sqrt{2}\right]$, hence $\aleph_0 = |\mathbb{Z}| \leq \left|\mathbb{Z}\left[\sqrt{2}\right]\right|$.
   Finally, by Cantor–Schröder–Bernstein theorem, we get that $\left|\mathbb{Z}\left[\sqrt{2}\right]\right| = \aleph_0$ as required.

Sample solutions to Exercise 6.

1. Since $|\mathbb{Q}| = |\mathbb{N}|$, there exists a bijective function $\psi : \mathbb{Q} \to \mathbb{N}$.
   We define $\Psi : \mathbb{R}^{\mathbb{N}} \to \mathbb{R}^{\mathbb{Q}}$ by $\Psi(f) = f \circ \psi$. Note that Ψ is bijective with inverse $\Psi^{-1}(g) = g \circ \psi^{-1}$.
   Indeed, for $f \in \mathbb{R}^{\mathbb{N}}$, $\Psi^{-1}(\Psi(f)) = f \circ \psi \circ \psi^{-1} = f$, and for $g \in \mathbb{R}^{\mathbb{Q}}$, $\Psi(\Psi^{-1}(g)) = g \circ \psi^{-1} \circ \psi = g$.
   Therefore $\left|\mathbb{R}^{\mathbb{Q}}\right| = \left|\mathbb{R}^{\mathbb{N}}\right| = |\mathbb{R}|$ by Week 11 Exercise 9.

2. Let $f, g \in C^0(\mathbb{R})$ be such that $\Phi(f) = \Phi(g)$, i.e. $f_{|\mathbb{Q}} = g_{|\mathbb{Q}}$ (*otherwise stated,* $\forall x \in \mathbb{Q},\ f(x) = g(x)$).
   Let $x \in \mathbb{R}$. By PS4, Exercise 3, there exists a sequence $(q_n)_n$ of rational numbers such that $\lim\limits_{n\to+\infty} q_n = x$.
   Then

$$\begin{aligned} f(x) &= \lim_{n\to+\infty} f(q_n) && \text{since } f \text{ is continuous} \\ &= \lim_{n\to+\infty} g(q_n) && \text{since } \forall n,\ q_n \in \mathbb{Q} \text{ and } f_{|\mathbb{Q}} = g_{|\mathbb{Q}} \\ &= g(x) && \text{since } g \text{ is continuous} \end{aligned}$$

   Therefore, $\forall x \in \mathbb{R},\ f(x) = g(x)$, so that $f = g$.

3. Since Φ is injective, we know that $\left|C^0(\mathbb{R})\right| \leq \left|\mathbb{R}^{\mathbb{Q}}\right| = |\mathbb{R}|$.
   Note that $\Gamma : \mathbb{R} \to C^0(\mathbb{R})$ mapping x_0 to the constant function

$$\Gamma(x_0) : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x_0 \end{array}$$

   is well-defined (since a constant function is continuous) and injective.
   Therefore $|\mathbb{R}| \leq \left|C^0(\mathbb{R})\right|$.
   From Cantor–Schröder–Bernstein theorem, we get that $\left|C^0(\mathbb{R})\right| = |\mathbb{R}|$.