# 21-373: FINAL EXAM

*With sample solutions*

**Name:** Anton Bernshteyn

Solve **exactly five** of the given problems. In the second column of the table below, write “Yes” or “No” next to each problem to indicate which five problems you wish to be graded.

<table>
<thead>
<tr>
<th>№</th>
<th>Graded?</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>/20</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>/20</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>/20</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>/20</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>/20</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>/20</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>/20</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>/100</td>
</tr>
</tbody>
</table>

No calculators, books, notes, &c. are allowed. Please justify all your answers.

**Good luck!**
Problem 1.

In this problem, $[0; 1)$ denotes the half-open unit interval that includes 0 but not 1.

For a real number $x \in \mathbb{R}$, let $x \pmod{1}$ denote the fractional part of $x$, i.e., the unique number $\alpha \in [0; 1)$ such that $x - \alpha$ is an integer. For $\alpha, \beta \in [0; 1)$, $r \in \mathbb{R}$, and $n \in \mathbb{Z}$, define

$$
\alpha \oplus \beta := (\alpha + \beta) \pmod{1},
\alpha \odot \beta := (\alpha \beta) \pmod{1},
\alpha \odot R \alpha := (r\alpha) \pmod{1},
n \cdot \mathbb{Z} \alpha := (n\alpha) \pmod{1}.
$$

(a) Is $([0; 1), \oplus)$ a group?
(b) Is $([0; 1), \oplus, \odot)$ a ring?
(c) Is $([0; 1), \oplus, \odot)$ a field?
(d) Is $([0; 1), \oplus, \odot \cdot \mathbb{Z})$ a $\mathbb{Z}$-module?
(e) Is $([0; 1), \oplus, \odot \cdot \mathbb{R})$ an $\mathbb{R}$-module (i.e., a vector space over $\mathbb{R}$)?

(a) **Answer:** Yes.

One could check directly that the group axioms are satisfied. A more slick approach is to observe that the structure $([0; 1), \oplus)$ is isomorphic to the quotient group $\mathbb{R}/\mathbb{Z}$, with the map $[0; 1) \to \mathbb{R}/\mathbb{Z}: \alpha \mapsto \alpha + \mathbb{Z}$ being an isomorphism.

(b) **Answer:** No.

Again, one can directly observe the failure of distributivity:

$$
\frac{1}{2} \odot \left( \frac{1}{2} \oplus \frac{1}{2} \right) = 0 \neq \frac{1}{2} = \left( \frac{1}{2} \odot \frac{1}{2} \right) \oplus \left( \frac{1}{2} \odot \frac{1}{2} \right).
$$

Alternatively, one can notice that if $([0; 1), \oplus, \odot)$ were a ring, then the map $\varphi: \mathbb{R} \to [0; 1): x \mapsto x \pmod{1}$ would have been a ring homomorphism; but $\ker \varphi = \mathbb{Z}$ is not an ideal in $\mathbb{R}$.

(c) **Answer:** No.

Follows from (b), since every field is in particular a ring.

(d) **Answer:** Yes.

For $\alpha \in [0; 1)$, let $\ominus \alpha$ denote the inverse of $\alpha$ in the group $([0; 1), \oplus)$. (Explicitly, $\ominus \alpha = 1 - \alpha$ for $\alpha \neq 0$, while $\ominus 0 = 0$.) It is not hard to see that for all $n \in \mathbb{N}$ and $\alpha \in [0; 1)$,

$$
n \cdot \mathbb{Z} \alpha = \underbrace{\alpha \oplus \cdots \oplus \alpha}_n \quad \text{and} \quad (-n) \cdot \mathbb{Z} \alpha = \underbrace{\ominus \alpha \oplus \cdots \oplus \ominus \alpha}_n.
$$

This means that the operation $\cdot \mathbb{Z}$ gives rise to the standard unital $\mathbb{Z}$-module structure on the Abelian group $([0; 1], \oplus)$. Alternatively, as in part (a), one can observe that $([0; 1), \oplus, \odot \cdot \mathbb{Z}) \cong \mathbb{R}/\mathbb{Z}$, where $\mathbb{R}$ is viewed as a unital $\mathbb{Z}$-module and $\mathbb{Z}$ is viewed as a submodule of $\mathbb{R}$.

(e) **Answer:** No.

The operation $\odot \mathbb{R}$ fails to be distributive:

$$
\frac{1}{2} \odot \mathbb{R} \left( \frac{1}{2} \oplus \frac{1}{2} \right) = 0 \neq \frac{1}{2} = \left( \frac{1}{2} \odot \mathbb{R} \frac{1}{2} \right) \oplus \left( \frac{1}{2} \odot \mathbb{R} \frac{1}{2} \right).
$$

Also, if $([0; 1), \oplus, \odot \cdot \mathbb{R})$ were a vector space over $\mathbb{R}$, then the map $\varphi: \mathbb{R} \to [0; 1): x \mapsto x \pmod{1}$ would be $\mathbb{R}$-linear (i.e., a vector space homomorphism); but $\ker \varphi = \mathbb{Z}$ is not a subspace of $\mathbb{R}$.
Problem 2.
Recall that an automorphism of a group \( G \) is a group isomorphism \( \varphi : G \to G \). The set of all automorphisms of \( G \) is denoted by \( \text{Aut}(G) \). Note that \( \text{Aut}(G) \) is itself a group under composition.

For each \( g \in G \), consider the conjugation map \( \text{conj}_g : G \to G : h \mapsto ghg^{-1} \). We know that \( \text{conj}_g \) is an automorphism of \( G \), so \( \text{conj}_g \in \text{Aut}(G) \). Such automorphisms are called inner automorphisms. The set of all inner automorphisms of \( G \) is denoted by \( \text{Inn}(G) \); that is,

\[
\text{Inn}(G) \coloneqq \{ \text{conj}_g : g \in G \} \subseteq \text{Aut}(G).
\]

(a) Show that \( \text{Inn}(G) \) is a normal subgroup of \( \text{Aut}(G) \).

(b) Show that if \( g, h \in G \) satisfy \( \text{conj}_h = (\text{conj}_g)^n \) for some \( n \in \mathbb{Z} \), then \( gh = hg \).

(c) Show that if the group \( \text{Inn}(G) \) is cyclic, then it is in fact trivial.

(d) Conclude that if the group \( \text{Aut}(G) \) is cyclic, then \( G \) is Abelian.

(a) The set \( \text{Inn}(G) \) is a subgroup of \( \text{Aut}(G) \) because the map \( G \to \text{Aut}(G) : g \mapsto \text{conj}_g \) is a group homomorphism and \( \text{Inn}(G) \) is its image. To see that the subgroup \( \text{Inn}(G) \) is normal, take any \( g \in G \) and \( \varphi \in \text{Aut}(G) \). We need to argue that \( \varphi \circ \text{conj}_g \circ \varphi^{-1} \in \text{Inn}(G) \). To this end, we shall prove that \( \varphi \circ \text{conj}_g \circ \varphi^{-1} = \text{conj}_{\varphi(g)} \). Indeed, for all \( h \in G \), we have

\[
(\varphi \circ \text{conj}_g \circ \varphi^{-1})(h) = (\varphi \circ \text{conj}_g)(\varphi^{-1}(h)) = \varphi(g\varphi^{-1}hg^{-1})
\]

[since \( \varphi \) is an isomorphism]

\[
= \varphi(g)\varphi(\varphi^{-1}(h))\varphi(g^{-1})
\]

\[
= \varphi(g)h\varphi(g)^{-1} = \text{conj}_{\varphi(g)}(h).
\]

(b) Suppose \( \text{conj}_h = (\text{conj}_g)^n \). Then

\[
ghg^{-1} = \text{conj}_h(g) = (\text{conj}_g)^n(g) = g^n gg^{-n} = g.
\]

This yields \( hg = gh \), as desired.

(c) Suppose \( \text{Inn}(G) = \langle \text{conj}_g \rangle \) for some \( g \in G \). Then for all \( h \in G \), \( \text{conj}_h = (\text{conj}_g)^n \) for some \( n \in \mathbb{Z} \). By part (b), we conclude that \( g \) commutes with every \( h \in G \). But this means that \( \text{conj}_g = \text{id}_G \), and hence the group \( \text{Inn}(G) \) is trivial.

(d) Every subgroup of a cyclic group is cyclic, so if \( \text{Aut}(G) \) is cyclic, then \( \text{Inn}(G) \) is cyclic as well. By part (c), this implies that \( \text{Inn}(G) \) is trivial, i.e., \( \text{conj}_g = \text{id}_G \) for all \( g \in G \). But \( \text{conj}_g = \text{id}_G \) if and only if \( g \) commutes with every element of \( G \). Thus, all elements of \( G \) commute with each other, i.e., \( G \) is Abelian.
Problem 3.

The infinite dihedral group $D_\infty$ is the subgroup of $\text{Sym}(\mathbb{Z})$ generated by the two bijections
\[ g: \mathbb{Z} \to \mathbb{Z}: n \mapsto n + 1 \quad \text{and} \quad h: \mathbb{Z} \to \mathbb{Z}: n \mapsto -n. \]

Show that the group $D_\infty$ is finitely presented (i.e., it has a presentation with finitely many generators and relations).

Let $\{x, y\}$ be a two-element set and let $\iota: \{x, y\} \to D_\infty$ be the map given by $\iota(x) := g$ and $\iota(y) := h$. We claim that $(D_\infty, \iota)$ is isomorphic to the group given by $\langle x, y \mid y^2, xyxy \rangle$. First, let us verify that $(D_\infty, \iota)$ satisfies the relations $y^2$ and $xyxy$: For all $n \in \mathbb{Z}$, we have
\[ h^2(n) = h(-n) = n; \]
\[ (g \circ h \circ g \circ h)(n) = (g \circ h \circ g)(-n) = (g \circ h)(-n + 1) = g(n - 1) = n. \]

Now suppose that $G$ is a group and $a, b \in G$ are elements such that $b^2 = abab = e_G$, where $e_G$ is the identity element of $G$. We have to show that there is a unique homomorphism $D_\infty \to G$ sending $g$ to $a$ and $h$ to $b$. The uniqueness of such a homomorphism (if it exists) follows from the fact that $D_\infty$ is generated by $g$ and $h$. So it remains to argue that such a homomorphism exists.

Without loss of generality, we may assume that $G$ is generated by $a$ and $b$ (otherwise we would pass to the subgroup $\langle a, b \rangle$). We claim that every element of $G$ can be written in the form $a^n b$ or $a^n b^m$ for some $n \in \mathbb{Z}$. Indeed, every element of $G$ can be written as a product of integer powers of $a$ and $b$. From $b^2 = e_G$, we obtain $b^{-1} = b$, and thus we may eliminate all the negative powers of $b$. Next, using that $abab = e_G$, we get $ba = a^{-1}b$ and $ba^{-1} = ab$. We can use these two equalities to eliminate the occurrences of $ba$ and $ba^{-1}$, thus moving all the powers of $b$ to the right of the powers of $a$. In this way, we express every element of $G$ in the form $a^n b^m$, where $n \in \mathbb{Z}$ and $m \in \mathbb{N}$. Finally, since $b^2 = e_G$, we may assume that $m \leq 1$, as desired. Exactly the same argument shows that every element of $D_\infty$ is of the form $g^n$ or $g^n \circ h$ for some $n \in \mathbb{Z}$.

We wish to define a function $\varphi: D_\infty \to G$ by sending each element of the form $g^{n_1} h^{n_2} \cdots h^{n_{2k}} \to a^{n_1} b^{n_2} \cdots a^{n_{2k-1}} b^{n_{2k}}$. (Here $n_1, \ldots, n_{2k}$ are integers, possibly 0.) Clearly, if such $\varphi$ is actually well-defined, then $\varphi$ is a desired homomorphism. To show that $\varphi$ is indeed well-defined, it suffices to argue that
\[ g^{n_1} h^{n_2} \cdots h^{n_{2k-1}} h^{n_{2k}} = \text{id}_\mathbb{Z}, \text{ then } a^{n_1} b^{n_2} \cdots a^{n_{2k-1}} b^{n_{2k}} = e_G. \]

Using the relations, we can write
\[ a^{n_1} b^{n_2} \cdots a^{n_{2k-1}} b^{n_{2k}} = a^n b^\ell, \]
for some $n \in \mathbb{Z}$ and $\ell \in \{0, 1\}$. The same sequence of reductions shows that
\[ \text{id}_\mathbb{Z} = g^{n_1} h^{n_2} \cdots h^{n_{2k-1}} h^{n_{2k}} = g^n h^\ell. \]

Then $0 = \text{id}_\mathbb{Z}(0) = (g^n h^\ell)(0) = n$, so $n = 0$, and $1 = \text{id}_\mathbb{Z}(1) = h^\ell(1) = (-1)^\ell$, so $\ell = 0$. Hence,
\[ a^{n_1} b^{n_2} \cdots a^{n_{2k-1}} b^{n_{2k}} = a^0 b^0 = e_G, \]
as desired.
Problem 4.

A ring $R$ is called a **Boolean ring** if for all $a \in R$, we have $a^2 = a$.

(a) Show that if $R$ is a Boolean ring and $a \in R$, then $a + a = 0$.

(b) Show that every Boolean ring is commutative.

(a) We have

$$a + a = (a + a)^2 = (a + a)(a + a) = a^2 + a^2 + a^2 + a^2 = (a + a) + (a + a).$$

Subtracting $a + a$ from both sides, we get $0 = a + a$, as desired.

(b) Take any $a, b \in R$ and write

$$a + b = (a + b)^2 = (a + b)(a + b) = a^2 + ab + ba + b^2 = (a + b) + (ab + ba).$$

Subtracting $a + b$ from both sides we get $0 = ab + ba$, i.e., $ab = -(ba)$. By part (a), $-(ba) = ba$, so we are done.
Problem 5.
On Midterm II, you established the following fact: If $G$ is a group and $g, h \in G$ are elements such that $|g|, |h| < \infty$ and $gh = hg$, then there is an element $s \in G$ with $|s| = \text{lcm}(|g|, |h|)$. You may freely use this fact in this problem.

(a) Show that if $G$ is a finite Abelian group, then there is an element $g \in G$ such that for all $h \in G$, the order of $h$ divides the order of $g$.

Given a field $K$, let $K^\times$ denote the multiplicative group of $K$; as a set, $K^\times := K \setminus \{0\}$, while the group operation on $K^\times$ is the multiplication in $K$. Since $K$ is a field, $K^\times$ is indeed a group (you do not have to prove this). For $a \in K^\times$, let $|a|$ denote the order of $a$ as an element of the group $K^\times$.

(b) Let $K$ be a finite field. Show that there is an element $a \in K^\times$ such that for all $x \in K^\times$, $x^{|a|} = 1$.

(c) Conclude that if $K$ is a finite field, then the multiplicative group $K^\times$ is cyclic.

(a) Let $g \in G$ be such that $|g|$ is maximum among all element of $G$ (such $g$ exists since $G$ is finite). Consider any $h \in G$. By the result from Midterm II, $G$ has an element $s$ with $|s| = \text{lcm}(|g|, |h|)$. By the choice of $g$, $|s| \leq |g|$, so $\text{lcm}(|g|, |h|) = |g|$, i.e., $|h|$ divides $|g|$, as desired.

(b) By part (a) applied to $G = K^\times$, there is $a \in K^\times$ such that for all $x \in K^\times$, $|x|$ divides $|a|$. Since $x^{|x|} = 1$, we conclude that $x^{|a|} = (x^{|a|})^{|x|/|a|} = 1^{|a|/|x|} = 1$ as well.

(c) Let $a \in K^\times$ be the element given by part (b). The polynomial $x^{|a|} - 1 \in K[x]$ has $|K^\times|$ distinct roots, namely all the elements of $K^\times$. Hence, its degree is at least $|K^\times|$, so $|a| \geq |K^\times|$. But the order of a group element cannot exceed the order of the group, so $|a| = |K^\times|$, which means that $K^\times$ is a cyclic group generated by $a$, as desired.
Problem 6.
Let $R$ be a commutative ring. An element $a \in R$ is **nilpotent** if there is some $n \in \mathbb{N}^+$ such that $a^n = 0$. Show that the set $N := \{a \in R : a \text{ is nilpotent}\}$ is an ideal in $R$.

First we show that for all $a \in N$ and $r \in R$, we have $ra \in N$. Indeed, suppose that $a^n = 0$. Then $(ra)^n = r^n a^n = r^n \cdot 0 = 0$ as well.

Now we need to show that $N$ is a subgroup of $(R, +)$. Clearly, $0 \in N$. Also, if $a \in N$, then $-a \in N$ as well, since if $a^n = 0$, then $(-a)^n = 0$ too. Finally, let $a, b \in N$ and suppose that $a^n = b^m = 0$ from some $n, m \in \mathbb{N}^+$. Then

$$(a + b)^{n+m-1} = \sum_{k=0}^{n+m-1} \binom{n+m-1}{k} a^k b^{n+m-k-1}.$$

For every $0 \leq k \leq n+m-1$, either $k \geq n$, or else, $n+m-k-1 \geq m$. In either case, $a^k b^{n+m-k-1} = 0$. Hence, $(a + b)^{n+m-1} = 0$ and so $a + b \in N$. 
Problem 7.
Let $K$ be a field and let $a \in K$. Let $I$ be the ideal in the polynomial ring $K[x]$ generated by the polynomial $x - a$. Show that there is a ring isomorphism $K[x]/I \cong K$.

We claim that the map $\varphi: K \to K[x]/I: c \mapsto c + I$ is a ring isomorphism. It is clear that this map is a homomorphism, since it is a composition of two homomorphisms:

$$K \to K[x] \to K[x]/I;$$
$$c \mapsto c \mapsto c + I.$$ 

It remains to show that this map is a bijection. The only ideals in the field $K$ are $\{0\}$ and $K$, so the kernel of $\varphi$ is either $\{0\}$ or $K$. Since this map is obviously nonzero, $\ker \varphi = \{0\}$, so $\varphi$ is injective. To prove surjectivity, take any element $p + I \in K[x]/I$, where $p \in K[x]$. We can divide $p$ by $x - a$ with remainder to get $p(x) = (x - a)q(x) + c$ for some $q \in K[x]$ and $c \in K$. But then $p(x) - c = (x - a)q(x) \in I$, so $p + I = c + I = \varphi(c)$, and we are done.
This page is intentionally left blank for use as scrap paper. If you want your work on this page to be graded, please indicate so clearly (including the problem number).
This page is intentionally left blank for use as scrap paper. If you want your work on this page to be graded, please indicate so clearly (including the problem number).
This page is intentionally left blank for use as scrap paper. If you want your work on this page to be graded, please indicate so clearly (including the problem number).
This page is intentionally left blank for use as scrap paper. If you want your work on this page to be graded, please indicate so clearly (including the problem number).
This page is intentionally left blank for use as scrap paper. If you want your work on this page to be graded, please indicate so clearly (including the problem number).
This page is intentionally left blank for use as scrap paper. If you want your work on this page to be graded, please indicate so clearly (including the problem number).