Math 202 / Problem Set 4 (two pages)

Basic facts about the arithmetic in \( \mathbb{N} \).

Recall the divisibility, \( d \mid n \) in \( \mathbb{N} \), and the definition of prime numbers \( p \) in \( \mathbb{N} \). Recall that \( (m,n) = \gcd(m,n) \) and \( [m,n] = \operatorname{lcm}(m,n) \) denote the greatest common divisor, respectively he lowest common multiple of \( m, n \). Recall what happens when \( m \) or \( n \) equal \( 0 \), and why it is meaningful to work with natural numbers in \( \mathbb{N}_{>0} \) when discussing divisibility. Make sure to review/know the following basic facts about the arithmetic in \( \mathbb{N} \).

- Let \( l + m = n \). Then \( k \) divides two of the numbers \( l, m, n \) if divides all three of them.
- Every natural number \( n \in \mathbb{N}_{>1} \) is a product of prime numbers.
- There are infinitely many prime numbers.
- Division with remainder: If \( m \neq 0 \), \( \exists q, r \in \mathbb{N} \) unique s.t. \( n = m \cdot q + r \), \( 0 \leq r < m \).
- There are unique primes \( p_1 < \cdots < p_r \) and \( e_1, \ldots, e_r > 0 \) s.t. \( n = p_1^{e_1} \cdots p_r^{e_r} \).
- Let \( m = p_1^{e_1} \cdots p_r^{e_r} \), \( n = q_1^{f_1} \cdots q_s^{f_s} \). Describe \( \gcd(m,n) \) and \( \operatorname{lcm}(m,n) \) in terms of the prime numbers \( p_i, q_j \) and their exponents \( e_i, f_j \) for \( 1 \leq i \leq r, 1 \leq j \leq s \).
- One has \( m \cdot n = \gcd(m,n) \cdot \operatorname{lcm}(m,n) \).

Equivalence relations Make sure that you check all the details of the fact that giving an equivalence relation \( \sim \) on a set \( A \) is the same as giving a partition \( A = \bigcup_i A_i \) of \( A \). Precisely:

- For equivalence classes \( \hat{x}, \hat{y} \) of \( \sim \) on \( A \), TFAE: (i) \( \hat{x} \cap \hat{y} \neq \emptyset \); (ii) \( \hat{x} = \hat{y} \); (iii) \( x \sim y \).

  In particular, the set of equivalence classes \( \hat{x} \) is a partition of \( A \) (WHY).

- If \( A = \bigcup_i A_i \) is a partition of \( A \), then: \( x \sim y \iff (\exists A_i \text{ s.t. } x, y \in A_i) \)

  is an equivalence relation on \( A \) such that \( \hat{x} = A_i \) provided \( x \in A_i \).

1) Let \( k \in \mathbb{N} \) be given. Define the relation \( \sim_k \) on \( \mathbb{N} \) by: \( m \sim_k n \iff (m \text{ and } n \text{ give the same remainder under division by } k) \). Prove/disprove/answer the following:

   a) \( \sim_k \) is an equivalence relation on \( \mathbb{N} \).

   b) What are the equivalence classes of 0, 1, \( k + 1 \), \( 3k + 2 \)?

The ring of integer numbers \( \mathbb{Z} \)

Recall that \( \mathbb{Z} = \mathbb{Z}/\sim := \mathbb{N} \times \mathbb{N}/\sim \) as defined in the class, and the definitions of the addition \( \oplus \) and the multiplication \( \odot \) on \( \mathbb{Z} \). Make sure that you know that \( \sim \) is an equivalence relation and that the addition \( \oplus \) and multiplication \( \odot \) are well defined (what does that mean?). Recall that each \( a = (m-n) \in \mathbb{Z} \) has a unique representative of the form: \( a = (k-0) =: k \in \mathbb{N} \) if \( m \geq n \), respectively \( a = (0-l) =: (-l) \in -\mathbb{N} \) if \( m \leq n \), where \( 0 = (-0) \). Hence \( \mathbb{Z} = -\mathbb{N} \cup \mathbb{N} \) with \((-0) = 0 \). Finally make sure that you know the notions:

- \( \mathbb{Z} \) endowed with \( \oplus \) is a commutative group (WHY).
- \( \mathbb{Z} \) endowed with \( \odot \) is a commutative monoid (WHY).
- \( \mathbb{Z} \) endowed with addition \( \oplus \) and multiplication \( \odot \) is a commutative ring (WHY).

2) Prove the following basic facts about the ring of integer numbers \( \mathbb{Z} \):

   a) \( \oplus \) and \( \odot \) on \( \mathbb{Z} \) have the cancelation property (what does that mean?).
b) $a, b \neq 0 \Rightarrow a \cdot b \neq 0$. If $a \cdot b = 1$, then either $a = 1 = b$, or $a = -1 = b$.

c) The sign rule $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$ holds in $\mathbb{Z}$.

3) Prove that $\mathbb{Z}, +, \cdot \text{ has no proper subrings}$, i.e., if $X \subset \mathbb{Z}$ is a subset which is closed with respect to the usual addition, subtraction, multiplication, and has $0_X, 1_X$, then $X = \mathbb{Z}$.

The field of rational numbers

Recall $\mathbb{Q} =: \mathbb{Q}/\sim := \mathbb{Z} \times \mathbb{Z}^* / \sim$ as defined in the class, and the definitions of the addition $+$ and the multiplication $\cdot$ on $\mathbb{Q}$. Make sure that you know that $\sim$ is an equivalence relation and that the addition $+$ and multiplication $\cdot$ are well defined (what does that mean?). Further, recall that every rational number $\frac{a}{r} - r_0 \in \mathbb{N}_{>0}$, $a_0 = n$ or $a_0 = -n$, with $n \in \mathbb{N}$ and $a, r_0$ relatively prime. Finally make sure that you know the notions:

- $\mathbb{Q}$ endowed with $+$ is a commutative group (WHY).
- $\mathbb{Q}^\ast$ endowed with $\cdot$ is a commutative group (WHY).
- $\mathbb{Q}$ endowed with addition $+$ and multiplication $\cdot$ is a field (WHY).

4) Prove that $\mathbb{Q}, +, \cdot \text{ has no proper subfields}$, i.e., if a subset $X \subset \mathbb{Q}$, $X \neq \{0\}$ is closed with respect to the usual addition, subtraction, multiplication, and division, then $X = \mathbb{Q}$.

5) Let $a = \frac{k}{r}, l \in \mathbb{N}_{>0}$ and $\text{g.c.d.}(l, k) = 1$. Prove the following:
   a) For $a = 15$ and $n = 7$, the equation $x^n = a$ has no solutions in $\mathbb{Q}$.
   b) The equation $x^n = a$ has a solution in $\mathbb{Q}$ iff both $k$ and any $l$ are $n$th powers in $\mathbb{N}$.

The canonical embeddings $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q}$ and the natural ordering.

From now on we denote the addition and multiplication in $\mathbb{Z}$ and $\mathbb{Q}$ simply by $+$ respectively $\cdot$ and recall the canonical embeddings $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q}$, defined by $n \mapsto (n-0) := n$, respectively $a \mapsto \frac{a}{r}$. Make sure that you know that the above embeddings are compatible with $+, \cdot$.

Concerning the natural ordering of $\mathbb{Z}$ and $\mathbb{Q}$, recall that:

- $\mathbb{Z}_{\geq 0} := \mathbb{N}$, and define: $a \leq b \iff b-a \in \mathbb{Z}_{\geq 0}$.
- $\mathbb{Q}_{\geq 0} := \left\{ \frac{k}{r} \mid k, l \in \mathbb{N}, l > 0 \right\}$, and define: $a \leq b \iff b-a \in \mathbb{Q}_{\geq 0}$.

6) Complete the proof of the assertions made in the class:
   a) $\leq$ are total orderings on both $\mathbb{Z}$ and $\mathbb{Q}$, compatible with $+$ and $\cdot$. (HOW).
   b) The canonical embeddings $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q}$ are compatible with the total orderings $\leq$.
   c) For all $a \in \mathbb{Q}$ one has: $a^2 \geq 0_{\mathbb{Q}}$, hence $a^2 > 0_{\mathbb{Q}}$ for $a \neq 0_{\mathbb{Q}}$.

The absolute value on $\mathbb{Z}$ and $\mathbb{Q}$.

Let $R$ denote either $\mathbb{Z}$ or $\mathbb{Q}$. Define $| | : R \rightarrow R_{\geq 0}$ by $|x| = x$ if $x \geq 0_R$, and $|x| = -x$ if $x \leq 0_R$. Then $| |$ is a well defined map (WHY), called the absolute value (map).

7) Prove that $| | : R \rightarrow R_{\geq 0}$ has the properties:
   a) $|a \cdot b| = |a| \cdot |b|$ for all $a, b \in \mathbb{Q}$.
   b) $|a + b| \leq |a| + |b|$ for all $a, b \in \mathbb{Q}$. For which $a, b \in \mathbb{Q}$ does one have: $|a + b| = |a| + |b|$?