Math 6020 / Problem Set 1 (two pages)

Basic facts about \( \mathbb{N}, \mathbb{Z}, \mathbb{Q} \)

1) Prove in all detail the following:
- If \( l + m = n \) in \( \mathbb{N} \) and \( k \) divides two of the numbers \( l, m, n \), then divides all three of them.
- Every natural number \( n > 1 \) is a product of prime numbers.
- **Division with remainder**: If \( m \neq 0, \exists q, r \in \mathbb{N} \) unique s.t. \( n = m \cdot q + r \), \( 0 \leq r < m \).
- **Euclidean Algorithm**: Let \( m, n \in \mathbb{N} \) with \( m \neq 0 \) nonzero, and set \( r_0 = n, r_1 = m \). For \( i \geq 1 \), define inductively, \( r_{i+1} \) as the remainder of division of \( r_{i-1} \) by \( r_i \). Then one has:
  (i) \( r_i = 0 \) for \( i \) sufficiently large.
  (ii) If \( i \geq 1 \) is maximal s.t. \( r_i \neq 0 \), then \( r_i = \gcd(m, n) \).
- Give an estimate of the number of operation to compute \( \gcd(m, n) \) in terms of \( m, n \).
- The set of prime numbers is infinite (“Euclid’s proof” Google it!).
- For \( n > 1 \) there are unique set distinct primes \( \Sigma_n = \{ p_1, \ldots, p_r \} \) and positive natural numbers \( n_p > 0 \) for \( p \in \Sigma_n \) s.t. \( n = \prod_{p \in \Sigma_n} p^{n_p} = p_1^{e_1} \cdots p_r^{e_r} \) with \( e_i = n_{p_i}, \ i = 1, \ldots, r \).
- For \( n, m > 1 \), let \( \Sigma_n, \Sigma_m \) and \( n_p \) for \( p \in \Sigma_n \) and \( m_p \) for \( p \in \Sigma_m \) be as above. Give the formula for \( \gcd(m, n) \) and \( \text{lcm}(m, n) \) in terms of \( \Sigma_n, \Sigma_m \) and \( n_p, m_p \) for \( p \in \Sigma_n \) and \( \Sigma_m \).

2) \( \mathbb{Z}, +, \cdot \) has no proper subrings, i.e., if is a subset \( X \subset \mathbb{Z} \) closed w.r.t. the usual addition, subtraction, multiplication, and has neutral elements \( 0_X \neq 1_X \), then \( X = \mathbb{Z} \).

3) \( \mathbb{Q}, +, \cdot \) 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 \( X = \mathbb{Q} \).

4) Prove/answer the following:
   a) \( \mathbb{Q} \) has no isolated elements, i.e., \( \forall a, b \in \mathbb{Q} \) one has: \( a < b \Rightarrow \exists c \in \mathbb{Q} \) s.t. \( a < c < b \).
   b) In particular, “most of the subsets” \( X \subset \mathbb{Q} \) are not well ordered. [WHY].
   c) Let \( X := \{ a \in \mathbb{Q} \mid a^2 < 2 \} \subset \mathbb{Q} \). Show that sup\((X)\), inf\((X)\) do not exist in \( \mathbb{Q} \).
   d) Let \( a \in \mathbb{Q}, a \neq -1, 0, 1 \) be fixed. Then there is \( n_0 \in \mathbb{N} \) such that the equation \( x^n = a \) has no solutions in \( \mathbb{Q} \) for \( n \in \mathbb{N}_{>n_0} \).

Composition laws & Basic algebraic structures

5) Let \( X \) be a non-empty set, and recall the **symmetric difference** \( A \triangle B := (A \setminus B) \cup (B \setminus A) \) on \( \mathcal{P}(X) \). Prove/answer the following:
   a) \( \mathcal{P}(X), \triangle, \cap \) is a commutative ring.
   b) Which elements in the ring \( \mathcal{P}(X), \triangle, \cap \) are invertible/zero divisors/nilpotent?
   c) Solve the equation \( x^2 + 1_{\mathcal{P}(X)} = 0_{\mathcal{P}(X)} \) in \( \mathcal{P}(X) \).

6) Let \( S_n \) be the symmetric group. Prove/disprove/answer the following:
   a) \( S_n \) is generated by the transpositions \( \sigma_{ij} \in S_n \), where \( \sigma(i) = j, \sigma(k) = k \) for \( k \neq i, j \)
   b) Solve the equations \( x \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \) and \( \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ x = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \) in \( S_3 \).
   c) Find the smallest \( n_G > 0 \) s.t. \( \sigma^{n_G} = e_G \) for all \( \sigma \in G \), where: i) \( G = S_6 \); ii) \( G = S_n \).
7) Denote i) $A_1A_2A_3$ triangles; ii) $B_1B_2B_3B_4$ parallelograms; iii) $C_1C_2C_3C_4C_5$ pentagons with three equal sides $|C_1C_2| = |C_2C_3| = |C_3C_4|$. Depending of further properties of these shapes, write in each case the group of transformations as permutation groups of the vertices, hence the results will be subgroups of $S_3$, $S_4$, $S_5$, respectively (why). [Note that the groups of transformations depend on the geometric properties of the shapes under discussion; e.g. in the case of triangles $A_1A_2A_3$, the group can be $\{(123),(132)\}$, $\{(123),(132)\}$, or $S_3$ (why), etc.]

8) Prove that in a finite ring $R$, $+, \cdot$ every $x \in R$ is either invertible or a zero divisor.

The rings $\mathbb{C}_R$ and $\mathbb{H}_R$ attached to a commutative ring $R$

Let $R$ be a commutative ring with $1_R \neq 0_R$, e.g. $R = \mathbb{Z}$, $R = \mathbb{Q}$, etc. Define the complexes $\mathbb{C}_R$ and the quaternions $\mathbb{H}_R$ over $R$ by $\mathbb{C}_R := R^2 := \{a + bi \mid a, b \in R\}$, respectively $\mathbb{H}_R := R^4 := \{a + bi + c_1j + d_\kappa \mid a, b, c, d \in R\}$, endowed with the coordinate-wise $+$ and the multiplication $\cdot$ defined by: $i^2 = j^2 = k^2 = -1_R$, $i \cdot j = k$, $j \cdot k = i$, $k \cdot i = j$. Define $\phi_C : R \to \mathbb{C}_R$, $a \mapsto (a, 0_R)$, $\phi_H : R \to \mathbb{H}_R$, $a \mapsto (a, 0_R, 0_R, 0_R)$, $\iota : \mathbb{C}_R \to \mathbb{H}_R$, $(a, b) \mapsto (a, b, 0_R, 0_R)$.

9) Prove/disprove the following:
   a) $\mathbb{C}_R, +, \cdot$ and $\mathbb{H}_R, +, \cdot$ are rings, $\mathbb{C}_R$ is comm., and $\mathbb{H}_R, +, \cdot$ is comm. iff $1_R = -1_R$.
   b) $\iota : \mathbb{C}_R \to \mathbb{H}_R$ maps $1_{\mathbb{C}_R}$ to $1_{\mathbb{H}_R}$ and is compatible with addition and multiplication.
   c) $\phi_C, \phi_H$ and map $1_R$ to $1_{\mathbb{C}_R}$, resp. $1_{\mathbb{H}_R}$ and are compatible with $+$ and $\cdot$ and $\phi_H(R)$ lies in the center of $\mathbb{H}_R$, i.e., $\phi_H(a) \cdot x = x \cdot \phi_H(a)$ $\forall a \in R$, $x \in \mathbb{H}_R$.
   d) Does $\iota(C_R)$ lie in the center of $\mathbb{H}_R$ as well?
   e) Let $R$ be a domain, and consider equations $x_1^2 + \cdots + x_k^2 = 0_R$ over $R$. One has:
   - $\mathbb{C}_R$ is a domain iff $x_1^2 + x_2^2 = 0_R$ has no non-trivial solution in $R$.
   - $\mathbb{H}_R$ has no non-trivial zero divisors iff $x_1^2 + \cdots + x_4^2 = 0_R$ has no non-trivial solutions.

Polynomials and formal power series

Given a commutative ring $R$ with $0_R \neq 1_R$, recall $R[t] \subset R[[t]]$ as introduced in class. Recall that the degree of polynomial $p = \sum_{n} a_n t^n \in R[t]$ is defined as follows: First, if $p = 0_R[t]$, then $\deg(p) = -\infty$ and second, if $p \neq 0_R[t]$, then $\deg(p) := \max\{n \mid a_n \neq 0_R\}$.

Terminology: If $p = \sum_a a_n t^n \neq 0_R[t]$ and $d = \deg(p)$, then $a_d$ is the leading coefficient of $p$.

10) Let $f = \sum_{n} a_n t^n \in R[[t]]$ and $p = \sum_{n} a_n t^n \in R[t]$ be given. Prove/disprove the following:
   a) (i) $f \in R[t]^x$ iff $a_0 \in R^x$. (ii) $p \in R[t]^x$ iff $a_0 \in R^x$ and $a_n, n > 0$ is nilpotent.
   b) $p$ is nilpotent iff all $a_n$ are nilpotent. Is the same true correspond. for $f \in R[[t]]$?

11) Prove the following:
   a) For $p, q \in R[t]$ one has: $\deg(p + q) \leq \max(\deg(p), \deg(q))$, $\deg(pq) \leq \deg(p) + \deg(q)$.
   Both for addition and/or multiplication, give sufficient condition such that “=” holds.
   b) The division with remainder holds as follows:
      Let $f, g \in R[t]$ and $g$ have invertible leading coefficient, in particular, $g \neq 0_R[t]$.
      Then there exist unique $p, r \in R[t]$ such that $f = gq + r$ and $\deg(r) < \deg(g)$.
   c) If $R = F$ is a field, the Euclidean algorithm holds in $F[t]$. (…last resort: Google it!)