Math 371 / Problem Set 3 (two pages)

Misellaneous (Groups & Rings)

Recall that every ring $R, + , \cdot$ with $0_R \neq 1_R$ and every (skew) field $F, + , \cdot$ have a unique minimal (w.r.t. $\subset$) subring $R_0 \subset R$, respectively subfield $F_0 \subset F$, called the prime subring of $R$, respectively the prime subfield of $F$ (and recall that $R_0$ and $F_0$ are generated by $\emptyset$). Let $\Sigma_R := \{ m \in \mathbb{N}_{>0} \mid m1_R = 0_R \}$, $\Sigma_F := \{ m \in \mathbb{N}_{>0} \mid m1_F = 0_F \}$. If $\Sigma_R, \Sigma_F \neq \emptyset$, set:
\[
m_R := \min \Sigma_R \quad \text{and} \quad p_F := \min \Sigma_F.
\]
Note: $m_F, p_F$ exist and $p_F$ is a prime number (Why).

1) In the above notation, let $\bullet \in \{ R, F \}$. Prove that the maps $i_\bullet$ below are isomorphisms:
   a) $i_R : \mathbb{Z} \rightarrow R_0$, $a \mapsto a1_R$, $i_F : \mathbb{Q} \rightarrow F_0$, $a \mapsto \frac{a}{p_F}1_R := (1/a1_F)$, provided $\Sigma_\bullet = \emptyset$.
   b) $i_R : \mathbb{Z}/m_R \mathbb{Z} \rightarrow R_0$, $\overline{a} \mapsto a1_R$, $i_F : \mathbb{Z}/p_F \mathbb{Z} \rightarrow F_0$, $\overline{a} \mapsto a1_F$, provided $\Sigma_\bullet \neq \emptyset$.
This give a complete description of the isomorphism types of prime rings/fields.

2) Let $G, \cdot$ be an arbitrary group. Prove/answer the following:
   a) For $g \in G$, define $i_g : G \rightarrow G$ by $x \mapsto g \cdot x \cdot g^{-1}$. Then $i_g \in \text{Aut}(G)$.
   b) $\text{Inn}(G) := \{ i_g \mid g \in G \} \triangleleft \text{Aut}(G)$ is a normal subgroup.
   c) The map $\iota : G \rightarrow \text{Inn}(G)$, $g \mapsto i_g$ is a group homomorphism. What is $\text{Ker}(\iota)$?

Terminology. The map $i_g$ is called the inner conjugation by $g$ on $G$.

The subgroup $\text{Inn}(G) \triangleleft \text{Aut}(G)$ is called the group of inner automorphisms in $G$.

The factor group $\text{Out}(G) := G/\text{Inn}(G)$ is the group of outer automorphisms of $G$.

3) Let $G, \cdot$ be an arbitrary group, and $g \in G$ be arbitrary. Prove/answer the following:
   a) The maps $l_g : G \rightarrow G$, $x \mapsto gx$ and $r_g : G \rightarrow G$, $x \mapsto xg^{-1}$ are bijective.
   b) For all $g, h \in G$ one has $l_g \circ l_h = l_{gh}$ and $r_g \circ r_h = r_{gh}$.
   c) The maps $\Psi_l : G \rightarrow \text{Bij}(G)$, $g \mapsto l_g$ and $\Psi_r : G \rightarrow \text{Bij}(G)$, $g \mapsto r_g$ are injective group homomorphisms.

Terminology. The maps $l_g$ and $r_g$ are called the left/right translation by $g$. Further, $\Psi_l$ and $\Psi_r$ are the standard left/right permutation representations of $G$. Therefore one has:

Every group $G$ has a canonical embedding $G \hookrightarrow \text{Bij}(G)$ in the group of bijections $\text{Bij}(G), \circ$.

4) Consider the multiplicative group $\mathbb{C}^\times$ of non-zero complex numbers and the multiplicative group of positive real numbers $\mathbb{R}_{>0}$ with respect to multiplication. Further let $| \cdot | : \mathbb{C}^\times \rightarrow \mathbb{R}_{>0}$ be the usual absolute value $|z| = \sqrt{a^2 + b^2}$ for $z = a + bi \in \mathbb{C}$. Prove/disprove the following:
   a) $| \cdot | : \mathbb{C}^\times \rightarrow \mathbb{R}_{>0}$ is a group homomorphism with $\text{Ker} \left( | \cdot | \right) = S := \{ z \in \mathbb{C} \mid |z| = 1 \}$.
   b) $\theta : \mathbb{C}^\times \rightarrow S$, $z \mapsto z/|z|$ is a group homomorphism with $\text{Ker}(\theta) = \mathbb{R}_{>0}$.

For $I = (a, b) \subset \mathbb{R}$ with $a < b$, set $I_Q := I \cap \mathbb{Q}$. Let $\mathcal{C}(I, \mathbb{R}) = \{ f \in \text{Maps}(I, \mathbb{R}) \mid f \text{ cont.} \}$. Define $\varphi : \text{Maps}(I, \mathbb{R}) \rightarrow \text{Maps}(I_Q, \mathbb{R}), f \mapsto f|_{I_Q}$ and $\varphi_C : \mathcal{C}(I, \mathbb{R}) \rightarrow \text{Maps}(I_Q, \mathbb{R}), f \mapsto f|_{I_Q}$.

5) In the above notation, prove/disprove/answer the following:
   a) $\mathcal{C}(I, \mathbb{R}) \subset \text{Maps}(I, \mathbb{R})$ is a subring.
   b) $\varphi$ and $\varphi_C$ are ring homomorphisms. What are $\text{Ker}(\varphi)$ and $\text{Ker}(\varphi_C)$?
6) Recalling the ring of modular arithmetic $\mathbb{Z}/m\mathbb{Z}$, $+, \cdot$ for $m \in \mathbb{N}_{>0}$, prove/answer:
   a) All the ideals of $\mathbb{Z}, +, \cdot$ are of the form $m\mathbb{Z}$ for some $m \in \mathbb{N}$.
   b) All the ideals of $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ endowed with coordinate-wise $+$ and $\cdot$ are of the form:
      \[ I = I_1 \times I_2 \text{ with } I_1 = m_1\mathbb{Z}, I_2 = m_2\mathbb{Z} \text{ ideals of } \mathbb{Z}, +, \cdot \]
   c) If so, then $\mathbb{Z}^2/I = \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ as product of rings.

7) **Chinese Remainder Theorem.** For $m, n \in \mathbb{N}_{>0}$ let $l := \text{lcm}(m, n)$. Prove/answer:
   a) $pr : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $a \mapsto (a/\sim_m, a/\sim_n)$ is a ring homomorphism with $\text{Ker}(pr) = l\mathbb{Z}$.
      Hence $\overline{pr} : \mathbb{Z}/l\mathbb{Z} = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $\overline{a} \mapsto pr(a)$ is well defined and injective (WHY). TFAE:
      (i) $\overline{pr}$ is surjective; (ii) $\overline{pr}$ is isomorphism; (iii) $\gcd(m, n) = 1$; (iv) $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$.
   b) For $m = 14$ and $n = 15$ find $a \in \mathbb{Z}$ such that $a \equiv 11 \pmod{14}$ and $a \equiv 10 \pmod{15}$.
   [Hint to b): Find $u_1, u_2 \in \mathbb{Z}$ with $pr(u_1) = (1, 0)$ and $pr(u_2) = (0, 1)$. Then $pr(xu_1 + yu_2) = (x, y)$ (WHY), etc.

To think about: What would/should be the assertion of the Chinese Remainder Thm for:
   a) Three numbers $k, m, n \in \mathbb{N}_{>0}$?
   b) Finitely many numbers $m_1, \ldots, m_\alpha \in \mathbb{N}_{>0}$?

8) Let $R = \mathbb{Z}/180\mathbb{Z}$. Answer the following:
   a) List all the zero divisors, reps. nilpotent elements, resp. all the ideals of $R$.
   b) Find all the roots of the degree one polynomial $\overline{t} = 15 \in R[t]$.
   c) Find all the polynomials $p(t) \in R[t]$ which are nilpotent, respectively invertible in $R[t]$.
   [Hint. Maybe use the Chinese Remainder Thm and write $R$ as a product simpler rings, etc...]

**Modules & Vector spaces**

9) For $M$ be a (left) $R$-module, review the proofs of the following assertion from the class:
   a) $r \cdot 0_M = 0_M = 0_R \cdot x \ \forall r \in R, x \in M$. If $r \in R^\times$ then $r \cdot x = 0_M$ iff $x = 0_M$.
   b) If $V$ is an $F$-vector space, and $a \in F$, $v \in V$, then: $a \cdot v = 0_V$ iff $a = 0_F$ or $v = 0_V$.

10) Let $R$ be a commutative ring with $0_R \neq 1_R$. Prove/answer the following:
   a) A subset $M \subset R$ is an $R$-submodule of $R$, + iff $M$ is an ideal of $R$.
   b) If $R$ is a field if an only if the $R$-submodules of $R$, + are $\{0_R\}$ and $R$ itself.
   c) An $R$-submodule $M$ of $R$, + is free iff $M = rR$ with $r \in R$ a non-zero divisor.

11) Prove/disprove the following:
   a) $\mathbb{Q}, +$ is not a finitely generated $\mathbb{Z}$-module.
   b) $\mathbb{R}, +$ is not a finitely generated $\mathbb{Q}$-vector space.
   c) $R[t], +$ is not a finitely generated $R$-module.

12) Let $R$ be a commutative ring, $X$ be an arbitrary non-empty set, and $\mathcal{F}(X, R)$ be the ring of all the $R$-valued maps on $X$ (w.r.t to the usual $+$ and $\cdot$ of maps). Prove/disprove/answer:
   a) $\mathcal{F}(X, R), +$ is finitely generated $R$-module if and only if $X$ is finite.
   b) If $X := \{x_1, \ldots, x_d\}$, give a basis of $\mathcal{F}(X, R), +$ as an $R$-module.
   c) Let $\text{Pol}_n(R) \subset R[t]$ be the $R$-module of polynomials of degree $\leq n$. Then $\mathcal{F}(X, R)$ and $\text{Pol}_n(R)$ are isomorphic $R$-modules iff $n = |X| + 1$. 

2