MATH 436: Homework IX.
Due on Wednesday, Nov 26

1. **Central Idempotents.** Let R be a ring (not necessarily commutative). We define the center of R and denote it by $Z(R)$ to be $Z(R) = \{z \in R | zr = rz \text{ for all } r \in R\}$.
(a) Show that $Z(R)$ is a commutative subring of R in general. Check that if $\alpha \in Z(R)$ then $(\alpha)_L = (\alpha)_R = (\alpha)$ i.e., the left ideal, right ideal and two-sided ideal generated by α all coincide. If F is a field, find the center of $Mat_n(F)$.
(b) If D is a division ring, show that $Z(D)$ is a field. Find the center of the division ring of quaternions $\mathbb{H}$.
(Note: We called the quaternions Q in a previous homework but we will now adopt the notation $\mathbb{H}$ which is more standard.)
(c) An element $\alpha \in R$ is called idempotent if $\alpha^2 = \alpha$. Show that if α is an idempotent of R then $1 - \alpha$ is also an idempotent of R. Show that in an integral ring, the only idempotents are 0 and 1.
(d) A decomposition of 1 into central idempotents is a decomposition $1 = e_1 + \cdots + e_n$ where $e_i \in Z(R)$ are nonzero and $e_i e_j = \delta_{ij} e_i$ for all $1 \leq i, j \leq n$. (Here δ_{ij} is Kronecker's delta symbol.) Define $R_i = (e_i)$ and check that R_i is a ring with identity e_i such that $R_i e_j = (0)$ for $j \neq i$. Show that $R_i \cap R_j = (0)$ for $1 \leq i \neq j \leq n$ and that $R_1 + R_2 + \cdots + R_n = R$. Conclude that every element $r \in R$ can be written uniquely as $r = r_1 + \cdots + r_n$ where $r_j \in R_j$ for all $1 \leq j \leq n$. Use this to construct an isomorphism of rings

$$R \cong \prod_{j=1}^{n} R_j$$

between R and the direct product of the rings R_j.

2. **Chinese Remainder Theorem via idempotents.** Let R be a ring.
(a) Suppose M and N are two sided ideals of R such that $M + N = R$ and $M \cap N = (0)$. Since $M + N = R$ we may write $1 = e_M + e_N$ for $e_M \in M$ and $e_N \in N$. Show that $e_M e_N = 0 = e_N e_M$ and use this to show that e_M and e_N are idempotents. Now use the defining relation $1 = e_M + e_N$ to show that e_M, e_N are central, $M = (e_M), N = (e_N)$. Thus by Exercise 1, we have an isomorphism of rings $R \cong M \times N$.

(b) Let M and N be two-sided ideals of R such that $M + N = R$. Let $a_M, a_N \in R$ be given. Consider the system of congruences:

$$\begin{aligned} x &\equiv a_M \bmod M \\ x &\equiv a_N \bmod N \end{aligned}$$

Show that there is an $x \in R$ which solves this system of congruences and that x is unique modulo $M \cap N$.
(Hint: Work in the quotient ring $R/(M \cap N)$ after explaining why part (a) applies to the images of M and N in that ring. Consider an expression of the form $x = a_M e_N + a_N e_M$ in R.)
(c) Let R be a ring and $M_1, \ldots, M_n$ be a collection of two-sided ideals of R. Suppose $M_i + M_j = R$ for all $1 \leq i \neq j \leq n$. For fixed i, j, explain why there exist elements $y_{ij} \in R$ such that

$$y_{ij} \equiv \begin{cases} 1 \bmod M_i \\ 0 \bmod M_j. \end{cases}$$

Use these to construct elements $y_i \in R$ such that

$$y_i \equiv \begin{cases} 1 \bmod M_i \\ 0 \bmod M_k \text{ for all } k \neq i. \end{cases}$$

Check that $x = y_1 a_1 + \cdots + y_n a_n$ is a solution to the system of congruences:

$$\begin{aligned} x &\equiv a_1 \bmod M_1 \\ x &\equiv a_2 \bmod M_2 \\ &\vdots \\ x &\equiv a_n \bmod M_n \end{aligned}$$

Show that x is unique modulo $M_1 \cap M_2 \cap \cdots \cap M_n$.
(d) Find the smallest positive integer x that solves the following system of congruences:

$$\begin{aligned} x &\equiv 3 \bmod 7 \\ x &\equiv 2 \bmod 8 \\ x &\equiv 5 \bmod 11. \end{aligned}$$

3. **Additive structure of Rings** Let R be a ring and $Unit(R)$ be its group of units. The additive group homomorphism $c : \mathbb{Z} \to R$ which sends 1 to 1 is easily checked to be a homomorphism of rings. The image $c(\mathbb{Z})$ is called the **characteristic subring** of R. Also $ker(c) = (d)$ for a unique nonnegative integer d which we call the **characteristic** of R. It is denoted $char(R)$.
(a) Check that if $char(R) = 1$ then $R = (0)$. If R is an integral ring then show that $char(R)$ is zero or a prime number.
(b) Show that if p is a prime and $char(R) = p$ then $(R, +)$ is an elementary abelian p-group and $|Unit(R)| \geq p - 1$. Show that if R is an integral ring of characteristic zero then $(R, +)$ is a torsion-free Abelian group and $|Unit(R)| \geq 2$.
(c) Suppose that $char(R) = ab$ where $a, b > 1$ are integers and $gcd(a, b) = 1$. Explain why $a, b \in Z(R)$ have $R = (a) + (b)$ and $(a) \cap (b) = (0)$. Conclude that there is a decomposition of 1 into central idempotents: $1 = e_a + e_b$ with $e_a \in (a), e_b \in (b)$ and hence conclude that there is an isomorphism of rings $R \cong (e_a) \times (e_b)$. Show that the additive order of e_a divides b and similarly the additive order of e_b divides a and use this to conclude that (e_a) is a ring of characteristic b and (e_b) is a ring of characteristic a.
(d) Let R be a ring of characteristic $n > 1$ and write $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ with $p_1 < \dots < p_k$ primes and $\alpha_j \geq 1$ for all j. Show that $R \cong R_1 \times \dots \times R_k$ where R_j is a ring of characteristic $p_j^{\alpha_j}$.
(e) Let p be a prime. Check that $\mathbb{Z}/p^k\mathbb{Z}$ is a ring of characteristic p^k which does not decompose into a direct product of two smaller rings.
(f) In an arbitrary ring R, show that $(a + b)^n$ is equal to a sum over all words of length n in a and b. Conclude that if a and b commute that $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is the usual binomial coefficient.
(g) If p is a prime, show that $\binom{p}{k}$ is an integer multiple of p for all $0 < k < p$. Thus conclude that in a ring of characteristic p, we have $(a + b)^p = a^p + b^p$ whenever a and b commute. (This is called the "Student's dream lemma".)

4. **Structure of UFDs.** We define $\oplus_{x \in X} \mathbb{N} \subset \oplus_{x \in X} \mathbb{Z}$ to be the submonoid of the free Abelian group on X which consists of tuples with nonnegative entries. It can be shown that $\oplus_{x \in X} \mathbb{N}$ is the free Abelian monoid on X. Let R be a UFD and R^* denote its nonzero elements. Let P be a set of representatives of the irreducibles of R up to the associate equivalence. Show that there is an isomorphism of monoids

$$(R^*, \cdot) \cong Unit(R) \times (\oplus_{p \in P} \mathbb{N}).$$

Here $\times$ stands for the direct product of monoids which is defined similarly to the direct product of groups.