Homework 11

1. Define the binomial coefficient $\binom{a}{b}$ to be
$$\frac{n!}{k!(n-k)!}$$
for integers $0 \leq k \leq n$. Let R be a commutative ring. We will prove the binomial theorem:
$$\forall a, b \in R\ \forall n \in \mathbb{N}, \qquad (a+b)^n = \sum_0^k \binom{n}{k} a^k b^{n-k}$$
We will prove by induction. First, clearly the formula holds for $n = 1$. Then assume the fomula holds for $(a+b)^n$, and we will show it is valid for $(a+b)^{n+1}$ as well.

We have
$$\begin{aligned}(a+b)^{n+1} = (a+b)^n(a+b) &= \left(\sum_0^n \binom{n}{k} a^k b^{n-k}\right)(a+b)\\ &= \sum_0^n \binom{n}{k} a^{k+1} b^{n-k} + \sum_0^n \binom{n}{k} a^k b^{n-k+1}\\ &= \sum_1^{n+1} \binom{n}{k-1} a^k b^{n-k+1} + \sum_0^n \binom{n}{k} a^k b^{n-k+1}\\ &= b^{n+1} + \sum_1^n \left(\binom{n}{k-1} + \binom{n}{k}\right) a^k b^{n+1-k} + a^{n+1}\\ &= b^{n+1} + \sum_1^n \binom{n+1}{k} a^k b^{n+1-k} + a^{n+1}\\ &= \sum_0^{n+1} \binom{n+1}{k} a^k b^{(n+1)-k}.\end{aligned}$$
as desired. The fact that $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ comes from the following calculation:
$$\begin{aligned}\binom{n}{k-1} + \binom{n}{k} &= \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!}\\ &= \frac{n!k}{k!(n-k+1)!} + \frac{n!(n-k+1)}{k!(n-k+1)!}\\ &= \frac{n!k + n \cdot n! - n!k + n!}{k!(n-k+1)!}\\ &= \frac{n!(n+1)}{k!(n-k+1)!} = \frac{(n+1)!}{k!((n+1)-k)!} = \binom{n+1}{k}\end{aligned}$$

2. Let R be a commutative ring of characteristic p for p prime. Consider the map $a \mapsto a^p$. We will prove this is a ring homomorphism.

Since R is commutative, we have $(ab)^p = a^p b^p$.

For addition, note that when k is not zero or p, the binomial coefficient $\binom{p}{k}$ is divisible by p. Then since R is characteristic p, we have
$$(a+b)^p = \sum_{k=0}^p \binom{p}{k} a^k b^{n-k} = a^p + b^p$$

verifying that the map is a ring homomorphism.

3. Let R be a commutative ring and let Z be the set consisting of all zero divisors and zero.

   The set of ideals contained in Z is ordered by set containment. Any linearly ordered subset has an upper bound, the union of the subset. Then by Zorn's lemma, there is an ideal M which is maximal with respect to containment amongst the set of all ideals contained in Z. We must show M is prime.

   Suppose not. Then there exist $a, b \in R$ such that $ab \in M$ but neither a or b is contained in M. Then the ideal $M + (a)$ is strictly larger than M, and the same for $M + (b)$. By maximality of M, there must exist elements $x \in M + (a)$ and $y \in M + (b)$ such that $x, y \notin Z$. Then we can write

$$x = m_1 + r_1 a, \quad y = m_2 + r_2 b,$$

   and their product

$$xy = m_1 m_2 + r_1 a m_2 + r_2 b m_1 + r_1 r_2 ab.$$

   Then $xy \in M$ since m_1, m_2, ab are each in M and M is an ideal. But then xy is a zero divisor, implying either x or y must be a zero divisor: if $c(ab) = 0$, then either ca is zero and a is a zero divisor, or ca is nonzero and b is a zero divisor. This is a contradiction. Thus M is a prime ideal contained in Z.

4. Let G be a finite group. We will show the center $Z(\mathbb{C}[G])$ of the group algebra $\mathbb{C}[G]$ has dimension equal to the number of conjugacy classes in G.

   To do this, we will give an explicit basis. For $g \in G$, define

$$e_{[g]} = \sum_{h \in G} hgh^{-1}.$$

   Note that for all $h \in [g]$, $e_{[h]} = e_{[g]}$. Then the number of elements $e_{[g]}$ is equal to the number of conjugacy classes in G. Let $N \subset G$ be a set containing one representative from each conjugacy class.

   We first show $e_{[g]} \in Z(\mathbb{C}[G])$ for all $g \in G$. Fix $g \in G$ and take any $a \in \mathbb{C}[G]$, with

$$a = \sum_{g \in G} a_g \cdot g$$

   for some $a_g \in \mathbb{C}$. We will show these elements commute. We have

$$e_{[g]} a = \sum_{h,k \in G} a_k \cdot hgh^{-1}k = \sum_{k \in G} \left(\sum_{h \in G} a_k hgh^{-1}k \right) = \sum_{k \in G} \left(\sum_{h \in G} a_k khgh^{-1}k^{-1}k \right) = \sum_{h,k \in G} a_k khgh^{-1},$$

   since the map $h \mapsto kh$ is a bijection of G, allowing us to interchange h with kh for a fixed k.

   Since the conjugacy classes of G are disjoint, if we have

$$\sum_{g \in N} a_g e_{[g]} = 0,$$

   it must be that $a_g = 0$ for all $g \in N$. Then $\{e_{[g]} : g \in N\}$ is a linearly independent set.

   Finally we will show these elements span $Z(\mathbb{C}[G])$. Suppose there is an element f which cannot be written as a linear combination of the $e_{[g]}$'s. Then f is not contstant on the conjugacy classes of G. Writing

$$f = \sum_{g \in G} f(g) \cdot g,$$

this means there exist $h, g \in G$ such that $f_(g) \neq f(hgh^{-1})$. Then consider the element $h = 1 \cdot h \in \mathbb{C}[G]$. We have

$$fh(hg) = f(hgh^{-1}),$$

but

$$hf(hg) = f(g).$$

Then $fh \neq hf$, meaning $f \notin Z(\mathbb{C}[G])$. By the contrapositive, every element in the center $Z(\mathbb{C}[G])$ is constant on the conjugacy classes of G. Then $Z(\mathbb{C}[G])$ is spanned by $\{e_{[g]} : g \in N\}$ and its dimension is equal to the size of this set, the number of conjugacy classes in G.

5. Let R be a ring and G be an infinite multiplicative cyclic group with generator ξ.