Homework Nine

1. The third isomorphism theorem for groups

In this problem, G need not be finite. Suppose $A \subset B \subset G$ are subgroups, and that $A, B \lhd G$. Building on last week's homework, exhibit an isomorphism

$$\psi : G/B \to (G/A)/(B/A).$$

You have proven the *third isomorphism theorem*. (And in case you're keeping count, don't worry—you haven't missed the second isomorphism theorem. We just haven't talked about it yet.)

2. Maps of quotients

Let A_1, A_2 and B_1, B_2 be abelian groups. Suppose we are given homomorphisms

$$\begin{array}{ccc} A_1 & \xrightarrow{i} & A_2 \\ \Big\downarrow{\scriptstyle f} & & \Big\downarrow{\scriptstyle g} \\ B_1 & \xrightarrow{j} & B_2 \end{array}$$

so that the above diagram commutes. This means that $gi = jf$ as group homomorphisms.

(a) Prove that the map sending $[a]$ to $[g(a)]$ is a well-defined group homomorphism from the quotient group $A_2/i(A_1)$ to the quotient group $B_2/j(B_1)$.

(b) Prove, *without using any formulas involving group elements* the existence and uniqueness of such a map. (Hint: Universal properties. You may use formulas involving equalities of functions, but don't ever write down elements of groups! It may help to give names to the homomorphisms $A_2 \to A_2/i(A_1)$ and $B_2 \to B_2/j(B_1)$.)

3. Polynomial rings and power series rings

Let R be a commutative ring. Let $R[[x]]$ be the set of power series with coefficients in R. Explicitly, an element of $R[[x]]$ is a power series

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots.$$

We may write this as

$$p(x) = \sum_{i=0}^{\infty} a_i x^i.$$

(As you're getting used to things, it may be useful for you to think of an element of $R[x]$ as equivalent information to an ordered sequence

$$(a_0, a_1, \ldots) \in R \times R \times \ldots$$

where each $a_i \in R$.)

If p and q are two power series with coefficients a_i and b_i, respectively, we define $p + q$ to be the power series whose ith coefficient is $a_i + b_i$. That is,

$$(p+q)(x) = \sum_{i \geq 0} (a_i + b_i) x^i.$$

We define the product power series to have kth coefficient given by

$$\sum_{i+j=k} a_i b_j.$$

That is,

$$(pq)(x) = \sum_{k \geq 0} (\sum_{i+j=k} a_i b_j) x^k.$$

Remark. As an explicit reminder, two power series $\sum a_i x^i$ and $\sum b_i x^i$ are equal if and only if $a_i = b_i$ for all i.

Remark. Also as a warning, note that there is no notion of convergence going on here. For instance, if the ring R is $\mathbb{Z}/n\mathbb{Z}$, there is no obvious way of talking about convergence of a power series. This is why—if you want to divorce the notion of power series in calculus from the formal algebraic manipulations we'll do here—it may help to now and then think of a power series simply as a sequence of elements of R.

(a) Prove that $R[[x]]$ is a commutative ring under the addition and product operations above.

Let $R[x] \subset R[[x]]$ be the subset of power series for which there exists some $n \in \mathbb{Z}_{\geq 0}$ such that $i > n \implies a_i = 0$. That is, $R[x]$ is the set of polynomials with coefficients in R.

(b) Show that the sum of two elements of $R[x]$ is again in $R[x]$, and likewise with products.
(c) Show that both the additive and multiplicative units of $R[[x]]$ are in $R[x]$.
(d) Explain why you've shown that $R[x]$ is a ring.

If $p(x)$ is not the zero polynomial, we call the largest i for which $a_i \neq 0$ the *degree* of the polynomial. If $p(x)$ *is* the zero polynomial, we will informally say that its degree is $-\infty$.

(e) Prove that $\deg(fg) = \deg f + \deg g$, with the obvious convention for what it means to add $-\infty$ to a number.

4. Modules as an abelian group with a ring action

Let M be an abelian group. An *endomorphism* of M is a group homomorphism from M to itself. Let $\mathrm{End}(M)$ denote the set of endomorphisms from M to itself. There are two operations

$$+ : \mathrm{End}(M)\times\mathrm{End}(M) \to \mathrm{End}(M) \qquad \text{and} \qquad \circ : \mathrm{End}(M)\times\mathrm{End}(M) \to \mathrm{End}(M)$$

The first is defined as follows: given two endomorphisms f and g, we obtain a third endomorphism $f + g$ by declaring

$$(f + g)(x) := f(x) + g(x)$$

for all $x \in M$. The second, $\circ$, is the usual composition of functions.
(a) Show that $\mathrm{End}(M)$ is an abelian group under the operation of adding functions. That is,
(b) Let $\circ$ denote the composition of functions. Show that $(\mathrm{End}(M), +, \circ)$ is a ring.
(c) Show that an R-module structure on M is the same thing as a ring homomorphism

$$R \to \mathrm{End}(M).$$

Philosophically, this is the same thing as saying that a group action on a set is the same thing as a group homomorphism

$$G \to \mathrm{Aut}(X).$$

There, $\mathrm{Aut}(X)$ consists of maps respects the property of *cardinality* of X. For modules, $\mathrm{End}(M)$ consists of maps respecting the structure of *additivity* of X.