Tutorial 3

Topic 1: Group Algebras. We have now done much of this in class.

1. Let R be a commutative ring, and let X be a set. The free R-module on X (also "*free R-module with basis X*"), denoted RX consists of all formal R-linear combinations of elements of X, equipped with the canonical addition and scalar multiplication. The standard example is R^n, the free module on n generators. Formulate and prove the universal property of RX. The universal property is as follows: Define the map

$$\begin{aligned} \eta : X &\longrightarrow RX \\ x &\longmapsto 1x. \end{aligned}$$

Then for any R-module M, we have a bijection

$$\begin{aligned} Hom_{R-Mod}(RX, M) &\stackrel{1-1}{\longleftrightarrow} Maps_{Sets}(X, M) \\ f &\longmapsto f \circ \eta \end{aligned}$$

To prove that this map is bijective, we note that η identifies X with a basis of RX. So, for any set map $\phi : X \to M$ there is one and only one R-linear extension, namely

$$f\left(\sum_{x\in X} a_x x\right) := \sum_{x\in X} a_x \phi(x).$$

2. Let R be a commutative ring, and let G be a group. In class we constructed the group algebra RG (also called $R[G]$). Prove that
   (a) specifying a ring homomorphism from $\mathbb{Z}G$ to S is equivalent to specifying a monoid homomorphism from G to $(S, \cdot)$. Indeed, it a straight forward to check that the one to one correspondence of Part 1 identifies ring homomorphisms with monoid homomorphisms.
   (b) the data of left RG-module are equivalent to the data of an R-module M together with an "R-linear G action", i.e., together with a group homomorphism

   $$\varrho : G \longrightarrow Aut_{R-Mod}(M).$$

   We break this into three steps:

i. **(Left-) modules over Algebras:** Let A be an R-algebra (see Tutorial 2), and let M be an A left-module. Then M is also an R-module, via the composition

$$R \longrightarrow A \longrightarrow End_{Ab}(M).$$

Conversely, an R-module M can be equipped with the structure of A left-module by specifying and R-bilinear multiplication

$$A \times M \stackrel{\cdot}{\longrightarrow} M.$$

Here R-bilinear means that for all $r \in R$, $a \in A$ and $m \in M$, we require $r(a \cdot m) = (ra) \cdot m = a \cdot (rm)$. We claim that specifying such an R-bilinear multiplication is equivalent to specifying an R-algebra homomorphism

$$\varrho : A \longrightarrow End_{R-Mod}(M).$$

Indeed, given the multiplication $\cdot$, we let $\varrho(a)$ be the R-module endomorphism sending m to $a \cdot m$. Conversely, given ϱ, we define the multiplication as $a \cdot m := \varrho(a)(m)$. It is a straightforward check (do it) that bilinearity of the multiplication translates into ϱ being an R-algebra homomorphism.

ii. We now apply this to the R-algebra RG. An RG left-module is an R-module M together with a ring homomorphism

$$RG \longrightarrow End_{R-mod}(M).$$

We may now argue as in Part (a) that for any R-algebra E, we have a bijection

$$\begin{array}{ccc} Hom_{R-Alg}(RG, E) & \stackrel{1-1}{\longleftrightarrow} & Maps_{Monoids}(G, E) \\ f & \longmapsto & f \circ \eta. \end{array}$$

Applying this to the endomorphism algebra $E = End_{R-Mod}(M)$, we have shown that a left-module M over RG is the same as an R-module M together with a monoid homomorphism

$$G \longrightarrow (End_{R-Mod}(M), \circ).$$

iii. Finally, let G be a group, and let H be a monoid. We will write $H^\times$ for the group of invertible elements in H. Then we have

$$Hom_{Monoids}(G, H) = Hom_{Groups}(G, H^\times).$$

Taking into account that the invertible endomorphisms are the automorphisms,

$$Aut_{R-Mod}(M) = End_{R-Mod}(M)^\times,$$

this completes the proof.

Topic 2: Ideals Let R be a commutative ring, and let $X \subset R$ be a subset.

1. Give a pedestrian (i.e., usable) definition of the ideal $\langle X \rangle$ of R generated by X. We claim that this ideal consists of all the (finite) R-linear combinations of elements in X:

$$\langle X \rangle = \left\{ \sum_{x \in X} a_x x \mid a_x \in R, |\{a_x \mid a_x \neq 0\}| < \infty \right\}.$$

Indeed, the right-hand side is an ideal containing X, so it also contains

$$\langle X \rangle = \bigcap_{X \subset I} I$$

where the intersection is over all ideals of R containing X. On the other hand, consider a finite linear combination $a = \sum a_x x$. Then every ideal I containing X also contains a. Hence a is also an element of the intersection of all these ideals, $a \in \langle X \rangle$.

2. What if R is not commutative? Similar to 1., but now the linear combinations are of the form

$$\sum_{x \in X} a_x x b_x$$

with a_x and b_x in R.

3. Familiarize yourself with the notion of a closure operator and list all the closure operators that have turned up in class to date.

A good place to start reading is `https://en.wikipedia.org/wiki/Closure_operator`, see also `https://en.wikipedia.org/wiki/Kuratowski_closure_axioms`. The examples you are familiar with are all the examples of sub-objects generated by a subset X, for instance, the span of a set of vectors inside a vector space V, the submodule generated by a set of elements of a module M, the ideal generated by a set of elements of a ring R (say commutative), the subgroup or the normal closure generated by a set of elements of a group G, etc. The formalism is always the same: a closure operator (also called hull operator)

$$cl : \mathcal{P}(Y) \longrightarrow \mathcal{P}(Y)$$

is determined by the set of hulls

$$\mathcal{H} := \{cl(X) \mid X \subseteq Y\}.$$

These are characterized axiomatically as follows: $\mathcal{H} \subset \mathcal{P}(Y)$ is a set of hulls if $Y \in \mathcal{H}$ and arbitrary intersections of elements of $\mathcal{H}$ are again in $\mathcal{H}$. In the examples above, $\mathcal{H}$ is, respectively, given by the set of subvectorspaces of the vector space $Y = V$, the set of submodules of the module $Y = M$ the set of ideals of the ring $Y = R$ the set of subgroups, respectively normal subgroups of the group $Y = G$. From $\mathcal{H}$, you recover the operator cl by setting

$$cl(X) := \bigcap_{X \subseteq A \in \mathcal{H}} A.$$

Then $cl(C)$ is an element of $\mathcal{H}$ containing X, and any element of $\mathcal{H}$ containing X also contains $cl(X)$. We have often used the notation $\langle X \rangle$ for $cl(X)$ and referred to this hull as the *subobject generated by* X. I believe that it is not a coincidence that we always have "pedestrian" definintions, obtained by applying all relevant operations to the elements of X (e.g., linear combinations, words, etc.). There is a theorem of universal algebra hiding here. But hull operators are a consept that is not limited to algebraic structures. There are other examples, such as the hull systems of convex sets in $\mathbb{R}^n$ or of closed sets in a topological space.

Topic 3: Field extensions 1. Show that every ring homomorphism whose source is a field is injective. This is not exactly true as stated. Let

$f : K \to R$ be a ring homomorphism, and assume that K is a field. We need make the additional assumption that $R \neq \{0\}$. Then we can conclude that $1 \neq 0$ in R: as soon as we know that there exists an element $a \neq 0$ in R, we have $1a = a \neq 0 = 0a$, hence $1 \neq 0$. To show that the kernel of f is $\{0\}$, assume that k is a non-zero element of K. Then $1 = f(1) = f(kk^{-1}) = f(k)f(k^{-1})$. If $f(k)$ was zero, it would follow that $1 = 0$, which is a contradiction to $R \neq \{0\}$.

2. Show that a commutative ring R is a field if and only if the only ideals in R are $\langle 0 \rangle$ and R. The *"only if"* part is a reformulation of Part 1., taking into account that ideals are exactly the kernels of ring homomorphisms. To show the *"if"* part, assume that R is a ring whose only ideals are $\langle 0 \rangle$ and R. Let $a \in R \setminus \{0\}$. We need to show that a is invertible. For this, we argue that the ideal generated by a is not the zero ideal, so we have $1 \in \langle a \rangle = R$. Using the pedestrian definition of $\langle a \rangle$, we conclude that 1 can be written as R-linear combination in a. In other words, there is an $r \in R$ with $ra = 1$.