University of Chicago, REU 2009: K-Theory

Peter May and Rina Anno

LECTURE 1

Tuesday, June 23

These notes were originally taken Monday, June 19, 2006 by Abigail Sheldon and TEXed by Jim Fowler. They were further edited in 2009 by Rolf Hoyer.

1. Monoids

DEFINITION 1.1. A **monoid** is a set M with

- an associative operation, i.e., a map $M \times M \to M$, written $(m, n) \mapsto mn$, satisfying
$$\forall m, n, p \in M,\ (mn)p = m(np),$$
- a two-sided identity, i.e., a distinguished element $e \in M$ satisfying
$$\forall m \in M,\ me = m = em.$$

We let the reader be warned that some use the term semigroup to denote a set with an associative operation but not necessarily an identity. Others use it synonymously with our definition of monoid.

DEFINITION 1.2. A monoid M is **commutative** or **abelian** if $mn = nm$ for all $m, n \in M$. We traditionally write commutative monoids additively instead of multiplicatively: i.e., we write 0 in place of e, and $m + n$ in place of mn.

EXAMPLE 1.3. The natural numbers $\mathbb{N} = \mathbb{Z}^{\geq 0}$ under addition form an abelian monoid, with zero as the identity. They also form an abelian monoid under multiplication, this time with one as the identity.

DEFINITION 1.4. A **group** is a monoid with inverses; i.e.,
$$\forall m \in M,\ \exists m^{-1} \in M,\ mm^{-1} = e = m^{-1}m.$$
A group is **abelian** if the underlying monoid is abelian.

We note that we view groups in two different, yet equivalent ways. We can either view it as a monoid for which every element has a two-sided inverse, or we can also view it as a monoid M equipped with an inversion function $\chi : M \to M$ (which we view as the map $m \mapsto m^{-1}$) with certain properties.

2. Maps of Monoids

DEFINITION 1.5. Let M, N be monoids, with $e_M \in M$ and $e_N \in N$ their respective identity elements. A function $f : M \to N$ is a **homomorphism of monoids** or simply a **map of monoids** if $f(e_M) = e_N$ and $\forall m, m' \in M$, $f(mm') = f(m)f(m')$.

DEFINITION 1.6. A homomorphism $f : M \to N$ is an **isomorphism** if there exists a homomorphism $f^{-1} : N \to M$ with $f \circ f^{-1} = f^{-1} \circ f =$ identity. Two monoids M and N are **isomorphic** if there exists an isomorphism $f : M \to N$.

For monoids, a bijective homomorphism is in fact an isomorphism. The desired inverse homomorphism will of course be the inverse as a set map, and it can be checked that this map is again a homomorphism of monoids.

REMARK 1.7. The analogous result is not true in other contexts. For instance if we have a continuous bijection between two topological spaces, the inverse function given as a set map need not be continuous

We note that we can now define a map of groups similarly to be any map between two groups preserving identity, products and inverses. However, this last condition is unecessary, meaning that maps of groups in this sense coincide with maps between groups that happen to be maps of monoids. To verify this claim, we let $f : G \to H$ be such a map, and check for any $g \in G$:

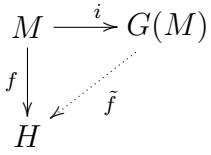
$$\begin{aligned} f(g)^{-1} &= f(g)^{-1}e_H \\ &= f(g)^{-1}f(e_G) \\ &= f(g)^{-1}f(gg^{-1}) \\ &= f(g)^{-1}f(g)f(g^{-1}) \\ &= f(g^{-1}) \end{aligned}$$

Thus, $f(g^{-1})$ gives the inverse element to $f(g)$, as desired.

3. Universal Properties

How can we construct a group from a monoid? We will call the group that we build from a monoid M the "group completion" of M.

DEFINITION 1.8. The **group completion** of M is a group $G(M)$ together with a map $i : M \to G(M)$ so that for all groups H and maps of monoids $f : M \to H$, there exists a *unique* $\tilde{f} : G \to H$ making the following diagram commute:

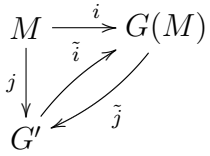


REMARK 1.9. To say that a diagram commutes means that the composition of maps from one object to another object doesn't depend on the route you take. In this case, the diagram commuting means that $\tilde{f} \circ i = f$.

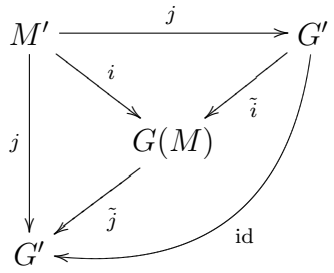
This definition is our first example of a **universal property**. It is critical that there exists a *unique* $\tilde{f}$.

Note that the group completion of M is more than just the group $G(M)$; it is also the map $i : M \to G(M)$, and the universal property implies that if the group completion exists, then $G(M)$ is unique up to (unique) isomorphism.

3.1. Uniqueness and Universal Properties. Suppose we have $j : M \to G'$ satisfying the same universal property as i and $G(M)$. Then we can construct unique maps $\tilde{i} : G' \to G(M), \tilde{j} : G(M) \to G'$ from the given universal property so that the following diagram commutes:



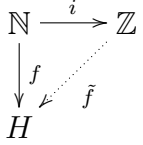
We now need only claim that $\tilde{i}, \tilde{j}$ are inverses to each other. This follows from another application of the universal property, as given in the following diagram:



Here we see that the smaller two triangles commute by the specification of $\tilde{i}, \tilde{j}$, so that the larger triangle commutes. However, the outer circuit involving the identity also commutes, trivially, so we conclude by uniqueness that the composite $\tilde{j}\tilde{i}$ is equal to the identity map of

G'. We conclude by a mirrored argument that $\tilde{i}\tilde{j}$ is the identity map of $G(M)$.

EXAMPLE 1.10. The group completion of $\mathbb{N}$ is $\mathbb{Z}$, because if H is a group and $f : \mathbb{N} \to H$ is any map of monoids, then defining $\tilde{f}(m-n) = f(m) - f(n)$ gives a well-defined map making the following diagram commute:



We have used additive notation for the multiplication in H, even though we did not assume that it is abelian. In fact, we can test the universal property for the group completion of an abelian monoid by mappings into abelian groups, because $\tilde{f}$ in the general case must land in an abelian subgroup of H.

In the previous example, we saw that $\mathbb{Z}$ was the group completion of $\mathbb{N}$ by explicitly checking that the universal property was satisfied. How can we know if we can do this in general? Does every monoid have a group completion? To explore questions like this, we need to provide a construction that will take a monoid, and produce a group G satisfying the universal property.

4. The First Construction

Our first construction of $G(M)$ will need to assume that M is abelian. We consider the set of pairs $\{(m, n) : m, n \in M\}$, thinking intuitively that (m, n) should represent "$m - n$." We define an equivalence relation $(m, n) \sim (m', n')$ if there exists some $q \in M$ such that $m + n' + q = m' + n + q$, which corresponds with our intuition, because if it were the case that $m - n = m' - n'$ then $m + n' = m' + n$ and furthermore $m + n' + q = m' + n + q$.

Let $[m, n]$ be the equivalence class of the pair (m, n), and let $G(M)$ be the set of all such equivalence classes. Define an operation on $G(M)$ by $[m, n] + [p, q] = [m + p, n + q]$.

We see that the class $[0, 0]$ acts as an identity, and observe that G is a monoid.

EXERCISE 1.11. Verify that $G(M)$ so defined is a monoid. In particular, check that our given operation is well-defined on equivalence classes.

In fact, $G(M)$ is a group, because

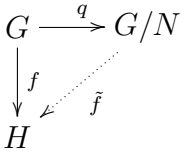
$$[m,n]+[n,m]=[m+n,n+m]=[m+n,m+n]=[0,0].$$

Thus we have constructed an abelian group $G(M)$ from an abelian monoid M. It remains to verify that $G(M)$ is the group completion of M. Define $i : M \to G(M)$ by setting $i(m) = [m, 0]$. Given a group H and a map $f : M \to H$, we define $\tilde{f}([m,n]) = f(m) - f(n)$ and we can check that this satisfies the appropriate universal property.

5. Review: Quotient Groups

Let G be a group, and $N \triangleleft G$, i.e., N is a normal subgroup in G, meaning that for any $g \in G$ and $n \in N$, the conjugate $gng^{-1} \in N$. We construct the **quotient group** G/N as the set of cosets $gN = \{gn : n \in N\}$, with the operation $gN \cdot hN = ghN$. There is a map $q : G \to G/N$ defined by $q(g) = gN$.

We can also define the quotient group by a universal property. The group G/N with $q : G \to G/N$ is the quotient group if the following is satisfied: for any group H and map $f : G \to H$ with $f(N) = e$, there exists a unique map $\tilde{f} : G/N \to H$ making the following diagram commute:

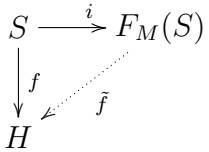


Definition 1.12. Let A, B be subgroups of a group G. The commutator $[A, B]$ subgroup is the subgroup generated by elements of the form $aba^{-1}b^{-1}$ for all $a \in A$ and $b \in B$.

6. Other Universal Properties

We give three more examples of universal properties.

Definition 1.13. The **free monoid** generated by a set S is a monoid $F_M(S)$ and a map of sets $i : S \to F_M(S)$ such that for any monoid N and map of sets $f : S \to N$, there exists a unique map of monoids $\tilde{f} : F_M(S) \to N$ making the following diagram commute:

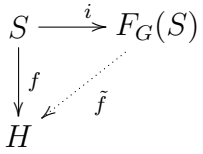


The set S need not be finite. To actually construct $F_M(S)$, we let our underlying set be the set of finite words in S, using the operation of concatenation. In other words, we have the following operation:

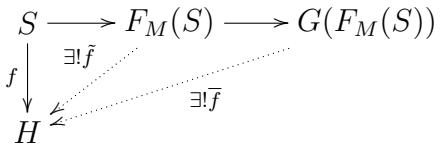
$$(s_1 s_2 \cdots s_n) \cdot (t_1 t_2 \cdots t_q) = s_1 s_2 \cdots s_n t_1 t_2 \cdots t_q$$

Given a set map $f : S \to N$, we see $\tilde{f}$ is forced to send a word $s_1 s_2 \cdots s_n$ to the product $f(s_1)f(s_2)\cdots f(s_n)$. This gives a map of monoids, and thus verifies the desired universal property.

DEFINITION 1.14. The **free group** generated by a set S is a group $F_G(S)$ and a map of sets $i : S \to F_G(S)$ such that for any group H and map of sets $f : S \to H$, there exists a unique map of groups $\tilde{f} : F_G(S) \to H$ making the following diagram commute:



We note that by examining the relevant universal properties, we see that $F_G(S)$ needs to coincide with $G(F_M(S))$ (assuming we know that such an object actually exists), by the following diagram:



The construction of $F_G(S)$ is similar to that of $F_M(S)$, in that we start with the words in S and formal inverses of elements of s. Thus, words are of the form $s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}$ with $s_i \in S, \epsilon_i = \pm 1$.

We have concatenation forming a product operation of the set of words, but we need to introduce an equivalence relation to complete our construction to get a group. Intuititively, our equivalence relation is based off of cancelling adjacent pairs of letters of the form ss^{-1} or $s^{-1}s$, giving meaning to the sense in which s, s^{-1} are formally inverse to each other.

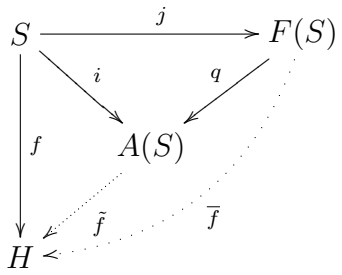
This equivalence relation will then respect our concatenation operation, and give us an inversion formula :

$$[s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}]^{-1} = [s_n^{-\epsilon_n} \cdots s_1^{-\epsilon_1}]$$

DEFINITION 1.15. The **free abelian group** generated by a set S is a group $A(S)$ and a map of sets $i : S \to A(S)$ such that for any *abelian* group H and map of sets $f : S \to H$, there exists a unique map of groups $\tilde{f} : A(S) \to H$ making the above diagram commute.

In some sense, these are the same universal property, but in different "worlds" of mathematics—the first in the "world" of groups, and the second in the "world" of abelian groups.

We will use $F(S)$ to construct $A(S)$. We claim that we can set $A(S) = F(S)/[F(S), F(S)]$. To see that this satisfies the universal property, consider the following diagram:



Here we have q as the quotient map, and i as the composite qj. We first observe that $\overline{f}$ (coming from the universal property of $F(S)$ and the map $f : S \to H$ considered as a set map) vanishes on $[F(S), F(S)]$ because for any $g, h \in F(S)$, we have the following noting again that H is abelian:

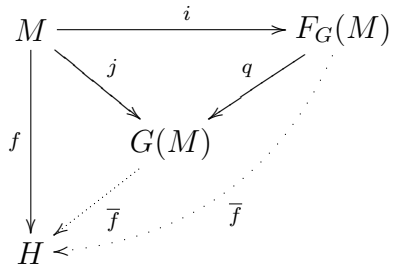
$$\begin{aligned} \overline{f}(ghg^{-1}h^{-1}) &= f(ghg^{-1}h^{-1}) = f(g)f(h)f(g^{-1})f(h^{-1}) \\ &= f(g)f(h)f(g)^{-1}f(h)^{-1} = f(g)f(g)^{-1}f(h)f(h)^{-1} = e \end{aligned}$$

Second, the universal property for quotient groups says that a map vanishing on $[F(S), F(S)]$ factors through the quotient $A(S)$, which provides the required $\tilde{f}$.

7. General Construction of the Group Completion

Here we provide a construction of $G(M)$ (now M need not be abelian) given by a quotient of $F_G(M)$. In particular, we set $G(M)$ to be the quotient of $F_G(M)$ generated by the normal subgroup generated by the elements $i(x)i(y)i(xy)^{-1}$, where $i : M \to F_G(M)$ is the given map. We define $j : M \to G(M)$ to be the composite of i and the quotient map $q : F_G(M) \to G(M)$. We obtain $\overline{f}$ using the universal

property of $F_G(M)$, and have the following diagram:



To get the desired $\tilde{f}$, we now note the following:

$$\begin{aligned}\overline{f}(i(x)i(y)(i(xy))^{-1}) &= \overline{f}i(x)\overline{f}i(y)(\overline{f}i(xy)))^{-1} \\ &= f(x)f(y)\left(f(xy)\right)^{-1} \\ &= e_H\end{aligned}$$

This shows that the generators of our normal subgroup all lie within the kernel of $\overline{f}$, and we get the desired $\tilde{f}$ by universal property of the quotient.

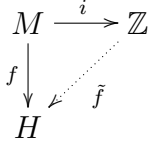
Here we see that elements of $G(M)$ can be characterized as equivalence classes of the form $[m_1^{\epsilon_1}]\cdots[m_n^{\epsilon_n}]$, where $m_i \in M, \epsilon_i = \pm 1$, and we make identifications of the form $[m_1 m_2] = [m_1 m_2]$.

This construction looks very different from the first construction—but since we proved the uniqueness of the group completion up to canonical isomorphism, in fact these two constructions give the same group.

EXAMPLE 1.16. Let $q \in \mathbb{N}$, and let x, y be formal variables. Define a set $M_q = \{0\} \cup \{mx : m \in \mathbb{N}\} \cup \{ny : n \in \mathbb{N}\}$ and an operation by the rules

$$\begin{aligned}0 + c &= c \\ mx + px &= (m+p)x \\ my + py &= (m+p)y \\ mx + ny &= (qm+n)y\end{aligned}$$

In fact, $x + y = (q+1)y$ implies $mx + ny = (qm+n)y$. Then M_q is a monoid, and $G(M_q) = \mathbb{Z}$. To verify this last fact, define $i : M \to \mathbb{Z}$ by $i(0) = 0$, $i(ny) = n$ and $i(mx) = qm$. Then to make the diagram



commute we need only define $\tilde{f}(n) = f(ny)$.

We could have explicitly constructed the group completion by using the first construction, but it is often easier to chase through universal properties than it is to chase through the details of a construction—and since verifying that the universal property holds is enough, relying on a universal property can often make for shorter, more concise proofs.

EXAMPLE 1.17. Look at the surfaces handout. The set of homeomorphism classes of surfaces is a monoid under the operation of connected sum. Let P be the projective plane, S the sphere, and T be the torus. Then S is the identity element, and

$$\begin{aligned} mP\#nP &= (m+n)P \\ mT\#nT &= (m+n)T \\ mP\#nT &= (m+2n)P \end{aligned}$$

so the set of surfaces under connected sum forms a monoid, which is isomorphic to the monoid M_2 from the previous example, and which therefore has group completion equal to $\mathbb{Z}$.

LECTURE 2

Wednesday, June 24

(These notes were written in 2009 by Claire Tomesch.)

1. Categories

DEFINITION 2.1. A **category** C consists of:

(1) A collection $\operatorname{ob} C$ whose elements are called *objects*;
(2) A collection $\operatorname{mor} C$ whose elements are called *morphisms* or *arrows*. Any $f \in \operatorname{mor} C$ has a unique *domain*, $\operatorname{dom}(f)$, and *codomain*, $\operatorname{cod}(f)$, which are both objects of C; if the domain of f is a and the codomain of f is b, we write $f : a \to b$ and say "f is an arrow from a to b." We denote the collection of morphisms from a to b in C by $C(a, b)$. We also require that for every $a, b \in \operatorname{ob} C$, $C(a, b)$ be a set.[1]
(3) For any pair $g, f \in \operatorname{mor} C$ such that $\operatorname{dom}(g) = \operatorname{cod}(f)$, we assign a *composite* $g \circ f$. More specifically, if $f \in C(a, b)$ and $g \in C(b, c)$, then $g \circ f \in C(a, c)$. We can write this more concisely as a function $\circ : C(b, c) \times C(a, b) \to C(a, c)$ called *composition*, defined for all triples of objects a, b, c. We think of composition diagramatically as

$$a \xrightarrow{f} b \xrightarrow{g} c \;=\; a \xrightarrow{g \circ f} c$$

We require composition to satisfy two axioms:
   (a) For given objects and morphisms

$$a \xrightarrow{f} b \xrightarrow{g} c \xrightarrow{h} d$$

   both ways of composing the maps result in the same thing; namely, one always has the equality $h \circ (g \circ f) = (h \circ g) \circ f$.
   (b) For every $b \in \operatorname{ob} C$, there is an *identity arrow* $1_b \in C(b, b)$ satisfying $1_b \circ f = f$ and $g \circ 1_b = g$ for all $f \in C(a, b)$ and $g \in C(b, c)$.

[1] This is not required for the definition to make sense; here we are restricting to what are called *locally small* categories.

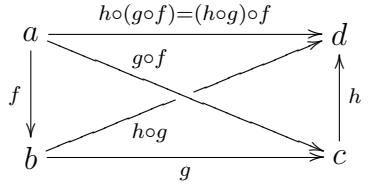
EXAMPLE 2.2. The most basic example is the category **Set**, whose objects are all sets and whose morphisms are all functions. Additionally, all the examples of algebraic structures and their homomorphisms that we've dealt with so far form categories:

(1) **Mon**, with objects all monoids and morphisms all homomorphisms of monoids;
(2) **AbMon**, with objects all abelian monoids and morphisms all homomorphisms of monoids;
(3) **Gp** with objects all groups and morphisms all homomorphisms of groups;
(4) **AbGp** with objects all abelian groups and morphisms all homomorphisms of groups.

EXAMPLE 2.3. There are many other smaller examples of categories. We can view any monoid as a category with one object and with morphisms all the elements of the monoid, with composition of morphisms given by the multiplication in the monoid. The identity of the monoid becomes the identity morphism on the one object, and the associativity of multiplication in the monoid encodes the associativity of composition.

We can also view any poset as a category, with objects the elements of the poset and a morphism $x \to y$ iff $x \leq y$ in the poset. On the other hand, any category C in which for all $a, b \in \operatorname{ob} C$, the hom-set $C(a, b)$ is either empty or a one-element set, is in fact a poset, by the same assignment: $a \leq b$ iff there exists an arrow $a \to b$.

REMARK 2.4. When we talk about morphisms in a category, instead of writing down equations, for example the associativity condition $h \circ (g \circ f) = (h \circ g) \circ f$, we will often draw diagrams like



The phrase "the diagram commutes" expresses that all the possible ways of composing all the arrows in the diagram (i.e. all the possible maximal paths along the arrows in the diagram) result in the same morphism.

2. Functors

DEFINITION 2.5. A (covariant) **functor** F from a category C to a category D consists of

(1) For every $a \in \operatorname{ob} C$, the assignment of an object $Fa \in \operatorname{ob} D$;
(2) For every pair of objects $a, b \in \operatorname{ob} C$, a function $F : C(a,b) \to D(Fa, Fb)$ taking a morphism $f : a \to b$ in C to a morphism $Ff : Fa \to Fb$ in D, satisfying the following conditions:
   (a) For every $a \in \operatorname{ob} C$, $F(1_a) = 1_{Fa}$;
   (b) For every pair of morphisms $f : a \to b$ and $g : b \to c$ in C, $F(g \circ f) = Fg \circ Ff$.

DEFINITION 2.6. A functor $F : C \to D$ is **faithful** if for every $a, b \in \operatorname{ob} C$, the function $F : C(a,b) \to D(Fa, Fb)$ is injective. A functor $F : C \to D$ is **full** if for every $a, b \in \operatorname{ob} C$, the function $F : C(a,b) \to D(Fa, Fb)$ is surjective.

EXAMPLE 2.7. A functor $F : C' \to C$ which is injective on objects and faithful defines C' as a *subcategory* of C. In this case, F is often called an inclusion functor. Since the collection of group homomorphisms between two groups coincides with the collection of monoid homomorphisms between them (Remark 1.7) – which can be expressed for any $G, H \in \operatorname{ob} \mathbf{Gp}$ as the equality $\mathbf{Gp}(G,H) = \mathbf{Mon}(G,H)$ – and every group is a monoid if we forget about inverses, we see that the "forgetful functor" $U : \mathbf{Gp} \to \mathbf{Mon}$ we considered before defines $\mathbf{Gp}$ as a subcategory of $\mathbf{Mon}$. The same is true if we consider the functor which "forgets" about abelianness: $\mathbf{AbGp}$ is a subcategory of $\mathbf{Gp}$, and $\mathbf{AbMon}$ is a subcategory of $\mathbf{Mon}$. These examples are all actually examples of *full* subcategories, where the inclusion functor also happens to be full.

EXAMPLE 2.8. Both of our group completion constructions form functors, $F : \mathbf{AbMon} \to \mathbf{Gp}$ and $F : \mathbf{Mon} \to \mathbf{Gp}$, respectively. The constructions we considered before give us a way of associating to every monoind M, a group $G(M)$, which defines the functor on objects. So we just need to define the functor on morphisms and check that it preserves composition and identities. Let $f : M \to N$ be a monoid homomorphism. Then consider the following diagram:

$$\begin{array}{ccc} M & \xrightarrow{i_M} & G(M) \\ {\scriptstyle f}\downarrow & & \\ N & \xrightarrow[i_N]{} & G(N) \end{array}$$

Since the composition $i_N \circ f$ is a homomorphism of monoids from M to $G(N)$, the universal property of $G(M)$ implies that there is a unique

homomorphism $G(f)$ of groups making the diagram commute:

$$\begin{array}{ccc} M & \xrightarrow{i_M} & G(M) \\ {\scriptstyle f}\downarrow & & \vdots\ {\scriptstyle \exists!\ G(f)} \\ N & \xrightarrow[i_N]{} & G(N) \end{array}$$

To check that this assignment preserves compositions, consider two composable monoid homomorphisms $f : M \to N$ and $g : N \to P$. By the above construction, the universal property of $G(M)$ and $G(N)$ yields $G(f)$ and $G(g)$, respectively. Thus we have a commutative diagram of the form:

$$\begin{array}{ccc} M & \xrightarrow{i_M} & G(M) \\ {\scriptstyle f}\downarrow & & \vdots\ {\scriptstyle \exists!\ G(f)} \\ N & \xrightarrow[i_N]{} & G(N) \\ {\scriptstyle g}\downarrow & & \vdots\ {\scriptstyle \exists!\ G(g)} \\ P & \xrightarrow[i_P]{} & G(P) \end{array}$$

However, $i_P \circ g \circ f$ is also a map of monoids from M to $G(P)$; thus the universal property of $G(M)$ gives us a unique group homomorphism $G(g \circ f)$ making the diagram commute:

$$\begin{array}{ccc} M & \xrightarrow{i_M} & G(M) \\ {\scriptstyle f}\downarrow & & \vdots \\ N & & \vdots\ {\scriptstyle \exists!\ G(g\circ f)} \\ {\scriptstyle g}\downarrow & & \vdots \\ P & \xrightarrow[i_P]{} & G(P) \end{array}$$

Thus, by the uniqueness given by the universal property of $G(M)$, we must have that $G(g \circ f) = G(g) \circ G(f)$, as desired. To see that this assignment preserves identities, just let $N = M$ and $f = 1_M$; then the universal property of $G(M)$ gives a commutative diagram:

$$\begin{array}{ccc} M & \xrightarrow{i_M} & G(M) \\ {\scriptstyle 1_M}\downarrow & & \vdots\ {\scriptstyle \exists!\ G(1_M)} \\ M & \xrightarrow[i_M]{} & G(M) \end{array}$$

However, the identity homomorphism $1_{G(M)} : G(M) \to G(M)$ also makes the diagram commute. Hence by uniqueness, we must have $G(1_M) = 1_{G(M)}$, as desired.

EXERCISE 2.9. Show that the construction of the free group on a set defines a functor $F : \mathbf{Set} \to \mathbf{Gp}$.

3. Natural Transformations

DEFINITION 2.10. Given two functors $F, G : C \to D$, a **natural transformation** $\eta : F \to G$ assigns to every object $a \in C$, a morphism $\eta_a : Fa \to Ga$ in D, such that for every morphism $f : a \to b$ in C, the following diagram commutes:

$$\begin{array}{ccc} Fa & \xrightarrow{Ff} & Fb \\ {\scriptstyle \eta_a}\downarrow & & \downarrow{\scriptstyle \eta_b} \\ Ga & \xrightarrow[Gf]{} & Gb \end{array}$$

EXAMPLE 2.11. The morphisms i_M from a monoid M to its group completion $G(M)$ fit together to form a natural transformation $i : 1_{\mathbf{Mon}} \to U \circ G$, where $1_{\mathbf{Mon}}$ is the identity functor on **Mon** and $U \circ G$ if the composition of the forgetful functor $U : \mathbf{Gp} \to \mathbf{Mon}$ and the group completion functor $G : \mathbf{Mon} \to \mathbf{Gp}$. (In the definition of the group completion, we are implicitly forgetting the group structure and only thinking of $G(M)$ as a monoid; hence, we've been abusing notion and writing $G(M)$ when we should have been writing $UG(M)$.)

EXAMPLE 2.12. Likewise, one can check that the morphisms i_S from a set S to the free group $F(S)$ on the set fit together to form a natural transformation $i : 1_{\mathbf{Set}} \to U \circ F$, where $1_{\mathbf{Set}}$ is the identity functor on **Set** and $U \circ F$ if the composition of the forgetful functor $U : \mathbf{Gp} \to \mathbf{Set}$ and the free group functor $F : \mathbf{Set} \to \mathbf{Gp}$.

4. Another Unversal Construction

Now we construct the free abelian monoid on a set. Let $S \in \operatorname{ob} \mathbf{Set}$. Define $F(S)$ to be finite formal sums of elements of S, for example $s_1 + s_1 + s_2 + s_1 + s_3 + s_4 + s_3$ for $s_1, s_2, s_3, s_4 \in S$. Since we can add two finite formal sums of elements to obtain another finite formal sum of elements, addition acts at the addition in $F(S)$, which is clearly associative. The empty formal sum acts as the identity.

Equivalently, $F(S)$ can also be constructed as the set of functions $f : S \to \mathbb{N}$ for which there are only finitely many elements $s \in S$ with $f(s) \neq 0$. The sum $f + g$ of two such functions $f, g : S \to \mathbb{N}$ is defined

for all $s \in S$ by $(f+g)(s) := f(s) + g(s)$. It is easy to see that the function $f + g : S \to \mathbb{N}$ also satisfies the condition that there are only finitely many $s \in S$ for which $(f+g)(s) \neq 0$, and that this definition of addition is associative. The function $0 : S \to \mathbb{N}$ taking every element of S to $0 \in \mathbb{N}$ acts as the identity.

There is yet another equivalent way to construct $F(S)$. Let S^n denote the cartesian product of n copies of the set S, and let Σ_n denote the permutation group on n letters. The elements of S^n are all the words of length n in the elements of S, so if we quotient by the equivalence relation $(s_1, s_2, \ldots, s_n) \sim (t_1, t_2, \ldots, t_n)$ if there exists a permutation $\pi \in \Sigma_n$ such that $s_i = t_{\pi(i)}$ for all $1 \leq i \leq n$, we obtain all words of length n in the elements of S where the elements of S are seen as formally commuting with one another. Denoting this quotient by S^n/Σ_n, we set $F(S) = \coprod_{n \in \mathbb{N}} S^n/\Sigma_n$. Defining the monoid operation in $F(S)$ to be concatenation of words, one can show that this is operation is well-defined on equivalence classes of words and is associative, with the empty word acting as the identity.

Exercise 2.13. Convince yourself that the above definitions are equivalent, i.e. for a fixed set S, they result in the same free abelian monoid $F(S)$. In each case, determine what the canonical function $i_S : S \to F(S)$ should be.

As usual, $F(S)$ with the canonical function $i_S : S \to F(S)$ satisfies the following universal property: Given a set S, an abelian monoid M and a function $f : S \to M$, there is a unique monoid homomorphism $\tilde{f} : F(S) \to M$ making the diagram commute:

$$\begin{array}{ccc} S & \xrightarrow{i_S} & F(S) \\ {\scriptstyle f}\downarrow & \swarrow_{\tilde{f}} \; {\scriptstyle \exists!} & \\ M & & \end{array}$$

Exercise 2.14. Using any one of the definitions, show that the free abelian monoid construction defines a functor $F : \mathbf{Set} \to \mathbf{AbMon}$.

5. Adjunctions

Definition 2.15. Given categories and functors

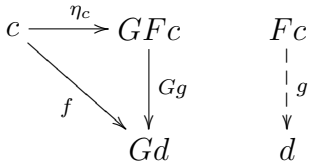
$$C \underset{G}{\overset{F}{\rightleftarrows}} D$$

and **adjunction** between F and G consists of a natural transformation

$$\eta : 1_C \to G \circ F$$

with the property:

(∗) For any objects $c \in \operatorname{ob} C$, $d \in \operatorname{ob} D$, and morphism $f : c \to Gd$, there exists a unique morphism $g : Fc \to d$ such that $f = Gg \circ \eta_c$ as indicated in



F is called the *left adjoint*, G the *right adjoint*, and η the *unit* of the adjunction. We say that F is *left adjoint* to G, which we write $F \dashv G$.

Remark 2.16. One can show that the above definition of adjunction is equivalent to requiring that for any $c \in \operatorname{ob} C$ and $d \in \operatorname{ob} D$, there be an isomorphism

$$\varphi_{c,d} : D(Fc, d) \cong C(c, Gd)$$

which is natural in c and d. Here, by "natural" we mean that, given any pair of morphisms $f : c' \to c$ in C and $g : d \to d'$ in D, the following diagram commutes:

$$\begin{array}{ccc} D(Fc, d) & \xrightarrow{D(Ff,g)} & D(Fc', d') \\ \downarrow{\scriptstyle \varphi_{c,d}} & & \downarrow{\scriptstyle \varphi_{c',d'}} \\ C(c, Gd) & \xrightarrow[C(f,Gg)]{} & C(c', Gd') \end{array}$$

where

$$D(Ff, g)(\ Fc \xrightarrow{q} d\ ) = \ Fc' \xrightarrow{Ff} Fc \xrightarrow{q} d \xrightarrow{g} d'$$

$$C(f, Gg)(\ c \xrightarrow{p} Gd\ ) = \ c' \xrightarrow{f} c \xrightarrow{p} Gd \xrightarrow{Gg} Gd'$$

We will clarify the contents of this remark in the next lecture.

LECTURE 3

Thursday, June 25

(These notes were written in 2009 by Claire Tomesch, based in part on notes from June 19, 2006 taken by Abigail Sheldon and TEXed by Jim Fowler.

1. Contravariant Functors and Opposite Categories

Before we can explore the many different equivalent definitions of adjunctions, we need some more terminology to be able to make precise what we hinted at in the final remark of yesterday's lecture.

DEFINITION 3.1. A **contravariant functor** $F : C \to D$ consists of:

(1) For every $a \in \operatorname{ob} C$, the assignment of an object $Fa \in \operatorname{ob} D$;
(2) For every pair of objects $a, b \in \operatorname{ob} C$, a function $F : C(a, b) \to D(Fb, Fa)$ taking a morphism $f : a \to b$ in C to a morphism $Ff : Fb \to Fa$ in D, satisfying the following conditions:
   (a) For every $a \in \operatorname{ob} C$, $F(1_a) = 1_{Fa}$;
   (b) For every pair of morphisms $f : a \to b$ and $g : b \to c$ in C, $F(g \circ f) = Ff \circ Fg$.

REMARK 3.2. Comparing this to the definition of (covariant) functor which we previously considered, one observes that a contravariant functor has all the same data except that it "reverses the direction of the arrows."

DEFINITION 3.3. Given a category C, the **opposite category** C^{op} is defined by setting

(1) $\operatorname{ob} C^{\mathrm{op}} := \operatorname{ob} C$; in words, C^{op} has the same objects as C;
(2) For all $a, b \in \operatorname{ob} C$, $C^{\mathrm{op}}(a, b) := C(b, a)$; in words, the arrows of C^{op} are the arrows of C but with the domain and codomain reversed.

REMARK 3.4. Thus a contravariant functor $F : C \to D$ is just a (covariant) functor $F : C^{\mathrm{op}} \to D$.

Now, we can make precise our previous remark. Given categories and functors

$$C \underset{G}{\overset{F}{\rightleftarrows}} D$$

the that condition for any $c \in \operatorname{ob} C$ and $d \in \operatorname{ob} D$, there is an isomorphism

$$\varphi_{c,d} : D(Fc, d) \cong C(c, Gd)$$

which is natural in c and d means that the $\varphi_{c,d}$ fit together to form a natural transformation

$$\varphi : D(F-, -) \to C(-, G-)$$

where

$$D(F-, -) : C^{\mathrm{op}} \times D \to \mathbf{Set}$$
$$C(-, G-) : C^{\mathrm{op}} \times D \to \mathbf{Set}$$

are functors defined on morphisms by the equations previously given: for morphisms $f : c' \to c$ in C and $g : d \to d'$ in D,

$$D(Ff, g)(\ Fc \xrightarrow{q} d\ ) = \ Fc' \xrightarrow{Ff} Fc \xrightarrow{q} d \xrightarrow{g} d'$$
$$C(f, Gg)(\ c \xrightarrow{p} Gd\ ) = \ c' \xrightarrow{f} c \xrightarrow{p} Gd \xrightarrow{Gg} Gd'$$

In this case, because each of the $\varphi_{c,d}$ is an isomorphism, such a φ is known as a *natural isomorphism.*

2. Adjunctions

We now prove that these different definitions of adjunction are in fact equivalent.

Proposition 3.5. *Given categories and functors*

$$C \underset{G}{\overset{F}{\rightleftarrows}} D$$

the following conditions are equivalent:

(1) *F is left adjoint to G, i.e. there exists a natural transformation*

$$\eta : 1_C \to G \circ F$$

with the property:

(∗) *For any objects* $c \in \operatorname{ob} C$, $d \in \operatorname{ob} D$, *and morphism* $f : c \to Gd$, *there exists a unique morphism* $g : Fc \to d$ *such that* $f = Gg \circ \eta_c$ *as indicated in*

$$\begin{array}{ccc} c & \xrightarrow{\eta_c} & GFc \\ & \searrow^{f} & \downarrow{\scriptstyle Gg} \\ & & Gd \end{array} \qquad \begin{array}{c} Fc \\ \vdots \\ \downarrow{\scriptstyle g} \\ d \end{array}$$

(2) *For any* $c \in \operatorname{ob} C$ *and* $d \in \operatorname{ob} D$, *there is an isomorphism*

$$\varphi_{c,d} : D(Fc, d) \cong C(c, Gd)$$

which is natural in c *and* d.

(3) *There are two natural transformations*

$$\eta : 1_C \to GF$$

$$\varepsilon : FG \to 1_D$$

respectively called the unit and the counit, such that the following diagrams of functors and natural transformations commute:

$$\begin{array}{ccc} F & \xrightarrow{F\eta} & FGF \\ & \searrow^{1_F} & \downarrow{\scriptstyle \varepsilon F} \\ & & F \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{\eta G} & GFG \\ & \searrow^{1_G} & \downarrow{\scriptstyle G\varepsilon} \\ & & G \end{array}$$

Proof. We only show the equivalence between (2) and (3), and leave the other equivalences as a (good!) exercise for the reader. To get from (2) to (3), for each $c \in \operatorname{ob} C$ and $d \in \operatorname{ob} D$, define

$$\eta_c := \varphi_{c,Fc}(1_{Fc})$$

$$\varepsilon_d := \varphi^{-1}_{Gd,d}(1_{Gd})$$

One can check that the naturality of φ implies that the above definitions fit together to form natural transformations η and ε, respectively. To see that these definitions make the above triangles commute, consider the following: by the naturality of φ, given any $f' : Fc \to d$, we have the following commutative diagram:

$$\begin{array}{ccc} D(Fc, Fc) & \xrightarrow{\varphi_{c,Fc}} & C(c, GFc) \\ {\scriptstyle D(1_{Fc}, f')}\downarrow & & \downarrow{\scriptstyle C(1_c, Gf')} \\ D(Fc, d) & \xrightarrow[\varphi_{c,d}]{} & C(c, Gd) \end{array}$$

But in this diagram, $1_{Fc} \in D(Fc, Fc)$ is mapped along the top and right to $Gf' \circ \eta_c$ and along the left and bottom to $\varphi_{c,d}(f')$. Since φ is a bijection, every morphism in $f \in C(c, Gd)$ can be written $f = \varphi_{c,d}(f') = Gf' \circ \eta_c$ for a unique $f' \in D(Fc, d)$. Now, let $c = Gd$ and $f' = \varepsilon_d$. Then the preceding equation implies that $\varphi_{Gd,d}(\varepsilon_d) = G\varepsilon_d \circ \eta_{Gd}$. But by definition, $\varepsilon_d = \varphi^{-1}_{Gd,d}(1_{Gd})$, and thus this becomes $1_{Gd} = G\varepsilon_d \circ \eta_{Gd}$, which exactly expresses the commutivity of

$$\begin{array}{ccc} G & \xrightarrow{\eta G} & GFG \\ & \searrow^{1_G} & \downarrow{\scriptstyle G\varepsilon} \\ & & G \end{array}$$

at the object d. One can show the commutivity of the other triangle in an exactly analogous manner (exercise!); thus (2) yields (3).

To go from (3) to (2), for each $f : Fc \to d$ and $g : c \to Gd$, define

$$\begin{aligned} \varphi_{c,d}(f) &:= Gf \circ \eta_c \\ \varphi^{-1}_{c,d}(g) &:= \varepsilon_d \circ Fg \end{aligned}$$

These are both natural tranformations by the naturality of η and ε. Now we need to show that they are actually inverse natural tranformations. To check this, we compute:

$$\begin{aligned} \varphi^{-1}_{c,d}\varphi_{c,d} f &= \varphi^{-1}_{c,d}(Gf \circ \eta_c) \\ &= \varepsilon_d \circ F(Gf \circ \eta_c) \\ &= \varepsilon_d \circ FGf \circ F(\eta_c) \\ &= f \circ \varepsilon_{Fc} \circ F(\eta_c) \\ &= f \circ 1_{Fc} \\ &= f \end{aligned}$$

and

$$\begin{aligned} \varphi_{c,d}\varphi^{-1}_{c,d} g &= \varphi_{c,d}(\varepsilon_d \circ Fg) \\ &= G(\varepsilon_d \circ Fg) \circ \eta_c \\ &= G(\varepsilon_d) \circ GFg \circ \eta_c \\ &= G(\varepsilon_d) \circ \eta_{Gd} \circ g \\ &= 1_{Gd} \circ g \\ &= g \end{aligned}$$

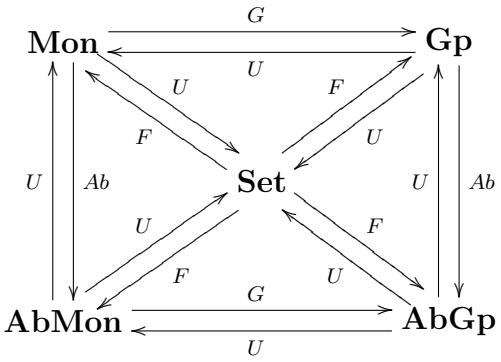
Hence $\varphi^{-1}\varphi = 1_{D(F-,-)}$ and $\varphi\varphi^{-1} = 1_{C(-,G-)}$, so $\varphi : D(F-,-) \to C(-,G-)$ is a natural isomorphism, completing the proof that (3) yields (2). $\square$

REMARK 3.6. The definition (2) is the reason why F is called the left adjoint and G is called the right adjoint.

EXERCISE 3.7. All of the pairs of corresponding free and forgetful functors we've considered form adjoint pairs, with free $\dashv$ forgetful, under the first definition. Using the preceding proposition, translate these adjuntions into the language of the other two definitions.

3. Abelianization

To complete[1] the diagram we have been secretly constructing and thinking about since the first lecture,



we construct the abelianization functor $Ab : \mathbf{Gp} \to \mathbf{AbGp}$.

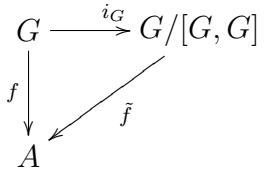
Let $G \in \mathbf{Gp}$. Then define the normal subgroup $[G, G] \lhd G$ to be the subgroup generated by the elements of the form $ghg^{-1}h^{-1}$ for all $g, h \in G$:

$$[G, G] := \langle ghg^{-1}h^{-1} \mid g, h \in G \rangle$$

$[G, G]$ is called the *conjugator subgroup* of G.

Define $Ab : \mathbf{Gp} \to \mathbf{AbGp}$ on objects by $Ab(G) := G/[G, G]$. Ab is defined on morphisms by the universal property of the quotient:

(∗) The quotient map $i_G : G \to G/[G, G]$ is universal in the sense that: given a morphism $f : G \to A$ of groups from G to an abelian group H, there is a unique map $\tilde{f} : G/[G, G] \to A$ making the diagram commute:



[1]Constructing the analogous functor for $Ab : \mathbf{Mon} \to \mathbf{AbMon}$ is one of the exercises.

The functors

$$\mathbf{Gp} \underset{U}{\overset{Ab}{\rightleftarrows}} \mathbf{AbGp}$$

again form an adjoint pair, with $Ab \dashv U$. The interesting thing to note in this case is that for $A \in \mathbf{AbGp}$, $Ab\,U\,A = A$.

4. Rings

DEFINITION 3.8. A **ring** R is a set together with two binary operations $+$ and $\cdot$ (called addition and multiplication) satisfying the following axioms:

(1) $(R, +)$ is an abelian group,
(2) $\cdot$ is associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$,
(3) The distributive laws hold in R: for all $a, b, c \in R$

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c) \quad \text{and} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

(4) R has an identity $1 \in R$ for $\cdot$: $a \cdot 1 = a = 1 \cdot a$ for all $a \in R$.

DEFINITION 3.9. A ring is *commutative* if its multiplication is commutative.

REMARK 3.10. In practice, we usually just write ab for $a \cdot b$ for $a, b \in R$. Also, in all that follows, we ignore the zero ring (where $0 = 1$); i.e. we only consider rings for which $0 \neq 1$.

EXAMPLE 3.11. $\mathbb{Z}$ is a ring with the usual addition and multiplication; any field is in fact a ring, so $\mathbb{R}$ and $\mathbb{C}$ are rings as well.

DEFINITION 3.12. Let R be a ring, I a subset of R and $r \in R$. Define

$$rI := \{ra \,|\, a \in I\} \quad \text{and} \quad Ir := \{ar \,|\, a \in I\}$$

The subset I of R is a **left ideal** if $(I, +)$ is a subgroup of $(R, +)$ and I is closed under left multiplication by elements of R, i.e. $rI \subset I$ for all $r \in R$. The subset I of R is a **right ideal** if $(I, +)$ is a subgroup of $(R, +)$ and I is closed under right multiplication by elements of R, i.e. $Ir \subset I$ for all $r \in R$. A subset I which is both a left and right ideal is called a (two-sided) **ideal**.

REMARK 3.13. For commutative rings, the notions of left, right and two-sided ideal coincide.

Let R be a ring and I a two-sided ideal in R. Then we can define an equivalence relation

$$a \sim b \quad \text{iff} \quad b - a \in I.$$

One can check that this relation respects the additive and multiplicative structure of R, and thus defines a congruence relation. When $a \sim b$, we say that a and b are *congruent modulo* I. The equivalence class of an element $a \in R$ is given by

$$a + I := \{a + i \,|\, i \in I\}$$

The set of all these equivalence classes is denoted R/I and becomes a ring if one defines

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I)(b + I) = ab + I$$

DEFINITION 3.14. Let R be a ring and I a two-sided ideal in R. Then R/I is the **quotient ring** of R modulo I.

EXAMPLE 3.15. Taking $R = \mathbb{Z}$, let $(p) := \{zp \,|\, z \in \mathbb{Z}\}$. One can check that for each $p \in \mathbb{Z}$, (p) is an ideal, so we have many examples of quotient rings: $\mathbb{Z}/(p)$.

DEFINITION 3.16. Let R be a ring.

(1) A nonzero element $a \in R$ is a *zero divisor* if there is a nonzero element $b \in R$ such that either $ab = 0$ or $ba = 0$.
(2) An element $u \in R$ is a *unit* if there exists some $v \in R$ such that $uv = vu = 1$. The set of units of R is denoted $R^\times$.

REMARK 3.17. Note that the collection of units $R^\times$ for a ring R forms a group under the multiplication of R.

5. Algebras and Modules

DEFINITION 3.18. Let R be a commutative ring. An **R-algebra** is a ring A together with a ring homomorphism $f : R \to A$ such that the image $f(R)$ is contained in the center of A.

DEFINITION 3.19. Let R be a ring. A **left R-module** is a set M together with

(1) a binary operation $+$ on M under which M forms an abelian group, and
(2) a map $R \times M \to M$ called an *action* of R on M, denoted by rm for all $r \in R$ and $m \in M$, satisfying
   (a) $(r + s)m = rm + sm$, for all $r, s \in R$ and $m \in M$,
   (b) $r(sm) = (rs)m$, for all $r, s \in R$ and $m \in M$,
   (c) $r(m + n) = rm + rn$, for all $r \in R$ and $m, n \in M$, and
   (d) $1m = m$, for all $m \in M$.

EXAMPLE 3.20. (1) Any ring is a module over itself.

(2) When $R = \mathbb{Z}$, an R-module is just an abelian group.
(3) When R is a field, vector spaces over that field are examples of modules.
(4) If A is an R-algebra, then A has a natural left and right R-module structure defined by $ra = ar = f(r)a$.

DEFINITION 3.21. Let R be a ring, I a set and $\{M_i \mid i \in I\}$ a collection of (left) R-modules. Then the **direct sum** of the M_i, denoted $\bigoplus_{i\in I} M_i$, is the R-module comprised of all finite R-linear combinations of the elements of the M_i. Explicitly, every element of $\bigoplus_{i\in I} M_i$ can be written

$$\sum_{j\in J} r_j m_j$$

for some finite subset $J \subset I$, where $r_j \in R$ and $m_j \in M_j$.

EXAMPLE 3.22. For a given ring R and set I, if we take $M_i = R$ for all $i \in I$, we obtain the free R-module on the set I. If we want to keep track of the factors, we often write $M_i = Ri$ instead, where $Ri = \{ri \mid r \in R\}$. This notion of free fits into the framework of our previous discussions.

6. The Group Ring and Related Notions

Let M be a monoid and R a ring. Define

$$R[M] := \bigoplus_{m\in M} Rm.$$

Then $R[M]$, in addition to being an R-module, is a ring:

$$\left(\sum_i r_i m_i\right)\left(\sum_j r_j m_j\right) = \sum_{i,j} r_i r_j (m_i m_j)$$

This induces a functor $R[-] : \mathbf{Mon} \to R\text{-}\mathbf{alg}$ which is left adjoint to the forgetful functor $U : R\text{-}\mathbf{alg} \to \mathbf{Mon}$. This construction results in something much more interesting when we consider groups instead of monoids.

DEFINITION 3.23. Let G be a group and R a ring. Define the **group ring** to be

$$R[G] := \bigoplus_{g\in G} Rg.$$

Then $R[G]$, in addition to being an R-module, forms a ring in the same way as in the monoid case already considered. This construction

induces a functor $R[-] : \mathbf{Gp} \to R\text{-}\mathbf{alg}$ which is left adjoint to the functor $(-)^\times : R\text{-}\mathbf{alg} \to \mathbf{Gp}$ taking an R-algebra to its group of units:

$$\mathbf{Gp} \underset{(-)^\times}{\overset{R[-]}{\rightleftarrows}} R\text{-}\mathbf{alg}$$

7. Rigs

DEFINITION 3.24. A **rig** (or *semiring*) T is a set together with two binary operations $+$ and $\cdot$ (called addition and multiplication) satisfying the following axioms:

(1) $(T, +)$ is an abelian monoid,
(2) $(T, \cdot)$ is a monoid,
(3) The distributive laws hold in T: for all $a, b, c \in T$

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c) \quad \text{and} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

(4) 0 is a zero: $0 \cdot a = a \cdot 0 = 0$.

REMARK 3.25. Thus a rig is really just a ring without additive inverses or, more commonly, without "negatives"; this is how the name rig is obtained from ring: just remove the "negatives."

8. Another Universal Construction

We can now mimic the completion construction we did to obtain a group from a monoid to obtain a ring from a rig.

DEFINITION 3.26. The **Grothendieck construction** on a rig T is a ring $G(T)$ together with a map $i_T : T \to G(T)$ such that for all rings H and morphisms of rigs $f : T \to H$, there exists a unique $\tilde{f} : G(T) \to H$ making the following diagram commute:

$$\begin{array}{ccc} T & \xrightarrow{i_T} & G(T) \\ {\scriptstyle f}\downarrow & \swarrow_{\tilde{f}} & \\ H & & \end{array}$$

We can construct the ring completion of any rig by applying the group completion to the abelian monoid $(T, +)$, and then noting that multiplication in T induces one in $G(T)$ for free. Looking back to our explicit construction of the group completion for an abelian monoid, since

$$(m - n) \cdot (p - q) = mp + nq - mq - np$$

we are led to define

$$[m, n] \cdot [p, q] = [mp + nq, mq + np].$$

One can check that this is well-defined on equivalence classes.

9. Burnside Ring

DEFINITION 3.27. Let G be a group. A **G-set** S is a set S with a map $G \times S \to S$, written $(g, s) \mapsto g \cdot s$, called an action of G on S, satisfying

(1) For all $s \in S$, $e \cdot s = s$,
(2) For all $g, h \in G$ and $s \in S$, $g \cdot (h \cdot s) = (gh) \cdot s$.

DEFINITION 3.28. Let S and T be G-sets. Then a **G-map** is a map $f : S \to T$ such that $f(g \cdot s) = gf(s)$ for all $g \in G$ and $s \in S$. A G-map is a *G-isomorphism* if there exists an inverse G-map.

Let $[S]$ denote the isomorphism class of the G-set S. We can turn the collection of isomorphism classes of finite G-sets into a rig as follows:

(1) Define $[S] + [T] = [S \sqcup T]$, where the G-action on $S \sqcup T$ comes from the G-action on S and T.
(2) Define $[S] \cdot [T] = [S \times T]$, where the G-action on $S \times T$ is the diagonal action, given by $g(s, t) = (gs, gt)$.
(3) Define $0 = [\emptyset]$.
(4) Define $1 = [*]$, where $*$ is a 1-point set with its unique (trivial) G-action.

One can check that this definition turns the set of isomorphism classes of finite G-sets into a rig.

DEFINITION 3.29. Define the **Burnside ring**[2] $A(G)$ of G, to be the Grothendieck construction on the rig of isomorphism classes of finite G-sets.

[2]Algebraists denote the Burnside ring by B(G), but topologists denote it $A(G)$; we follow the latter convention.

LECTURE 4

Friday, June 26

(These notes were written in 2009 by Rolf Hoyer, based in part on notes taken in 2006 by Jim Fowler)

1. A few more words about $A(G)$

For a finite group G, we recall that were can put a semiring (or "rig" for ring without negatives) structure on the isomorphism classes of finite G-sets via the operations of disjoint union and cartesian product. We apply the Grothendieck construction and the result is denoted the Burnside ring $A(G)$.

DEFINITION 4.1. Let G be a group, and H a subgroup of G. An **orbit** is the G-set $G/H = \{gH : g \in G\}$ of cosets, with the G-action $G \times G/H \to G/H$ given by $(k, gH) \mapsto kgH$.

Given x an arbitrary element of some G-set S, we can examine the orbit $Gx = \{gx : g \in G\}$. This is isomorphic as a G-set to G/H_x, where $H_x = \{h \in G : ghx = x\}$ denotes the **stabilizer**, or **isotropy group** of x. Here the isomorphism is given by $gx \mapsto gH$. We can now look at some $y \notin Gx$, and continuing in this matter we can partition all of S into such orbits. We have now demonstrated the following:

PROPOSITION 4.2. *Any finite G-set is isomorphic to the disjoint union $\coprod_{i=1}^{n} G/H_i$ of orbits.*

We now note that for subgroups H, K of G we have $G/H, G/K$ isomorphic as G-sets if and only if they are conjugate, meaning that $H = gKg^{-1}$ for some $g \in G$. This map corresponds to the isomorphism of G-sets, which must be of the form $g'H \mapsto g'gK$. This yields the following:

COROLLARY 4.3. *The underlying group of the Burnside ring $A(G)$ is the free abelian group generated by elements $[G/H]$ as H ranges across conjugacy classes of subgroups of G*

Thus, the additive structure of $A(G)$ is easily computed. We note that the multiplicative structure is much more difficult, since it takes

some work to express the product $G/H \times G/K$ as a disjoint union of orbits.

To demonstrate an application of Burnside rings, we need the following definitions:

DEFINITION 4.4. A **simple group** is a nonabelian group G with no normal subgroups other than 0 and G.

DEFINITION 4.5. A finite group G is **solvable** if there exists subgroups $G_0, \ldots, G_s$ such that

$$G \triangleright G_s \triangleright G_{s-1} \triangleright \cdots \triangleright G_0 = \{e\}$$

and G_i/G_{i-1} is cyclic of prime order.

The Feit-Thompson Theorem asserts that any group G of odd order is solvable. In particular, it shows that no group of odd order is simple. It can be rephrased in terms of the Burnside ring $A(G)$.

DEFINITION 4.6. An **idempotent** in a ring R is an element $x \in R$ such that $x^2 = x$.

All rings trivially have at least two idempotents, given by 0 and 1.

EXAMPLE 4.7. In the product ring $R = R_1 \times R_2$, nontrivial idempotents include $e_1 = (1, 0)$ and $e_2 = (0, 1)$.

The following result now holds:

THEOREM 4.8. *The group G is solvable if and only if $0 = [\emptyset], 1 = [*]$ are the only idempotents in $A(G)$.*

From this we now see that the Feit-Thompson Theorem is equivalent to demonstrating that 0 and 1 are the only idempotents in $A(G)$ if G is of odd order.

2. Group representations

We let R be some ring, and recall that a (left) R-module M is an abelian group M equipped with a R-bilinear map $R \times M \to M$.

We recall that a free R-module of the form $R[S]$ is given by elements of the form $\sum_{i=1}^{n} r_i s_i$. If S is a G-set we then have that $R[S]$ is an $R[G]$-module, with the action given by

$$\left(\sum_i r_i g_i\right)\left(\sum_j r'_j s_j\right) = \left(\sum_{i,j} r_i r'_j g_i s_j\right)$$

DEFINITION 4.9. An **R-representation** of G is an isomorphism class of (left) R-modules.

Isomorphism classes of the given form $[R[S]]$ are called **permutation representations** since the action of G permutes the basis elements of the free R-module $R[S]$.

We see that this definition might yield a similar structure to the Burnside ring, since we have a well-defined addition given by direct sum. The isomorphism $R[S] \oplus R[T] \cong R[S \coprod T]$ shows that this respects our already-existing addition on isomorphism classes of G-sets.

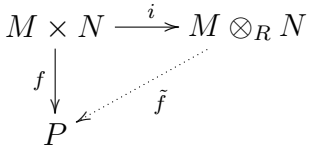
3. Tensor products

To get a corresponding multiplication, we desire an operation that would take the pair $R[S], R[T]$ to $R[S \times T]$.

Cartesian products will prove to be too awkward for this purpose. The natural construction will yield an R-bilinear map $R[S] \times R[T] \to R[S \times T]$. However, we note that for $s \in S, t \in T$, we have $r(s,t) = (rs, rt)$ on the left mapping to r^2 times the generator (s,t) on the right, so this map is not a map of R-modules, let alone a candidate for isomorphism. Our goal in this section is to somehow interpret R-bilinear maps as maps of R-modules.

For the rest of the lecture, we will assume that R is a commutative ring for the sake of simplicity. (If we didn't do this, we'd have to let M be a right R-module, N be a left R-module. Then the resulting construction would yield an Abelian group without an R-module structure)

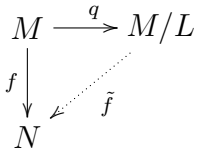
Definition 4.10. For R-modules M, N, the **tensor product** of M and N, denoted $M \otimes_R N$, is an R-module equipped with a map $i : M \times N \to M \otimes_R N$ with the following universal property: Given an R-bilinear map $M \times N \to P$, there exists a unique map $\tilde{f}$ such that the following diagram commutes:



Definition 4.11. An R-**submodule** $L \subset M$ of an R-module M is a subgroup L preserved by the action of R, so that $rl \subset L$ for all $r \in R, l \in L$.

The natural R-module structure on the group quotient M/L yields an R-module M/L with the following universal property: if $f : M \to N$ is a map of R-modules satisfying $f(L) = 0$, then there exists a map

$\tilde{f} : M/L \to N$ such that the following diagram commutes:



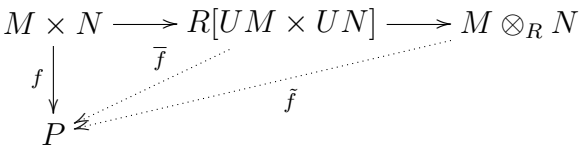
We note R-bilinearity of a map f is given by the following conditions

$$\begin{aligned} f(m+m',n) &= f(m,n)+f(m',n) \\ f(m,n+n') &= f(m,n)+f(m,n') \\ f(rm,n) &= rf(m,n) = f(m,rn) \end{aligned}$$

Our construction of the tensor product is now to set $M \otimes_R N = R[UM \times UN]/J$, where U is the functor giving the underlying set of a given R-module, and J is the R-submodule generated by elements of the form

$$\begin{array}{cc} (m+m',n)-((m,n)+(m',n)), & (m,n+n')-((m,n)+(m,n')) \\ (rm,n)-r(m,n) & (m,rn)-r(m,n) \end{array}$$

The universal property is verified by the following diagram:



The map $\overline{f}$ exists uniquely from the universal property of free R-modules over a set. We see directly from the R-bilinearity of f that $\overline{f}$ vanishes on the generators of J , and then $\tilde{f}$ then exists uniquely by the universal property of quotient modules.

Our map $M \times N \to M \otimes_R N$ is given by sending (m,n) to the equivalence class $m \otimes n$ containing the generator of the copy of R corresponding to (m,n). The map $M \times N \to N \otimes_R M$ sending (m,n) to $n \otimes m$ then induces an isomorphism $M \otimes_R N \cong N \otimes_R M$.

In the case $M = R[S], N = R[T]$, we see that an R-bilinear map $R[S] \times R[T] \to P$ is determined uniquely by the images of (s,t) for basis elements $s \in S, t \in T$. This verifies the desired isomorphism $R[S] \otimes_R R[T] \cong R[S \times T]$.

4. The Representation ring

We assume G a finite set and R is a commutative ring, but note that we emphasize the cases $R = \mathbb{R}, \mathbb{C}$, so our modules are in fact vector spaces.

We claim that the set of group representations is a commutative semiring (or "rig"), with operations $[V] + [W] = [V \otimes W], [V] \cdot [W] = [V \otimes_R W]$. We see that $V \otimes_R W$ is a $R[G]$-module if we let G act diagonally, so that $g(v \otimes w) = gv \otimes gw$. The additive and multiplicative identities are given by $0 = [0], 1 = [R]$, where $[R]$ is given the trivial G-action. (We omit the proof of the distributive law $(M \oplus N) \otimes_R P \cong (M \otimes_R N) \oplus (N \otimes_R P)$)

Definition 4.12. The **representation ring** of G is the ring obtained by applying the Grothendieck construction to the semiring of isomorphism classes of R-representations of G, under direct sum and tensor product. In the cases $R = \mathbb{C}, \mathbb{R}$, these are denoted $R(G), RO(G)$, respectively. The formal inverses $-[M]$ arising from this construction are known as **virtual representations**

Our verification $R[S \coprod T] \cong R[S] \oplus R[T], R[S \times T] \cong R[S] \otimes_R R[T]$ demonstrates the existence of a ring homomorphism $A(G) \to R(G)$ induced by the map $[S] \mapsto [\mathbb{C}[S]]$, where $\mathbb{C}[S]$ is given the permutation action of G on basis elements.

Any $\mathbb{R}$-module V can be used to construct a $\mathbb{C}$-module. The structure is given by $V \otimes_{\mathbb{R}} \mathbb{C}$, with action given by $z(v \otimes w) = v \otimes zw$. This construction is known as **extension of scalars**. We note that $\mathbb{R}[S] \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}[S]$ for any set. Applying this to the case of $\mathbb{R}[G]$ modules shows that the following diagram commutes:

$$\begin{array}{ccc} A(G) & \longrightarrow & RO(G) \\ & \searrow & \downarrow{\scriptstyle -\otimes_{\mathbb{R}}\mathbb{C}} \\ & & R(G) \end{array}$$

We refer to a result that helps classify isomorphism classes of representations:

Theorem 4.13 (Maschke). *Let R be either $\mathbb{R}$, $\mathbb{C}$, or any finite field $\mathbb{F}_q$, where $q = p^r$ and p does not divide the order of G. Then every finite-dimensional R-representation of G breaks uniquely into the direct sum of irreducibles, where a representation is irreducible if has no nontrivial $R[G]$-submodules.*

This immediately implies the following:

COROLLARY 4.14. *The underlying group of $R(G)$ is the free abelian group generated by elements $[M]$ as M ranges across the isomorphism classes of irreducible R -representations of G.*

It is a fact (over $\mathbb{C}, \mathbb{R}$) that every isomorphism class of irreducible representations occurs as a summand of the **regular representation** given by G acting on $\mathbb{C}[G]$ by left-multiplication on basis elements.

EXERCISE 4.15. Using the given facts, compute $R(G), RO(G)$ when G is a cyclic of order p. Then, compute $A(G)$ and the given maps into the representation rings.

LECTURE 5

Tuesday, July 7

(These notes were written in 2009 by Rolf Hoyer,
with image macros provided by Rina Anno)

1. Braid Groups

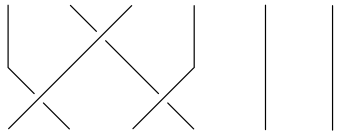


FIGURE 1. Example of a braid

We intuitively seek to define a group whose elements consist of some number of **threads**. These threads are start and end at some number of fixed points at the bottom and top, respectively, of our mental picture. In the middle we allow our threads to twist . It is easy to visualize a binary operation on such pictures, given by attaching the bottom of one to the top of another.

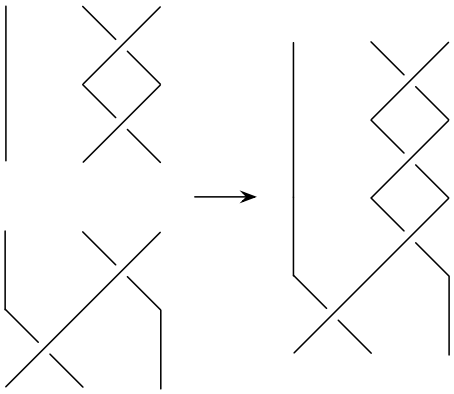


FIGURE 2. Example of braid composition

DEFINITION 5.1. A **braid** is collections of n disjoint **threads**, which are maps $[0,1] \to \mathbb{R}^3$. These threads are required to send 0 to the set $\{(k,0,0) : k = 1,\dots,n\}$ and to send 1 to the set $\{(k,0,1) : k = 1,\dots,n\}$. We also require that the z-coordinate of each thread be an increasing function $[0,1] \to \mathbb{R}$.

The threads of a braid then all lie between the planes $z = 0$ and $z = 1$. If we have two braids, we can translate the threads of the second to lie between the planes $z = 1$ and $z = 2$. If f is a thread of the first braid ending at $(k,0,1)$ and g is a thread beginning at $(k,0,1)$, we can attach the two and get a map of the form:

$$h(x) = \begin{cases} f(2x) & \text{for } x \in [0,1/2] \\ g(2x-1) + (0,0,1) & \text{for } x \in [1/2,1] \end{cases}$$

This does not yield a valid thread, since the new endpoints are now the set $\{(k,0,2) : k = 1,\dots,n\}$. To get a thread we therefore scale the z-coordinate of our map $h(x)$ by a factor of one-half.

However, this operation does not preserve associativity. Given braids B_1, B_2, B_3, we see that $(B_1B_2)B_3$ contains a compressed version of B_1 in the time interval $[0,1/4]$, and we see that B_2 and B_3 are similarly compressed into the intervals $[1/4,1/2]$ and $[1/2,1]$. However, in the $B_1(B_2B_3)$ the corresponding intervals are instead $[0,1/2]$, $[1/2,3/4]$, and $[3/4,1]$. We wish to identify these two braids with one another, so we introduce the following concept:

DEFINITION 5.2. Two braids B_1 and B_2 are **isotopic** if there exists a map $\{[0,1] \sqcup \cdots \sqcup [0,1]\} \times [t_1,t_2] \to \mathbb{R}^3$ such that the map given by restriction to the subspace $\{[0,1] \sqcup \cdots \sqcup [0,1]\} \times \{t\}$ is a braid for each $t \in [t_1,t_2]$, such that B_1 is the braid at time t_1 and B_2 is the braid at time t_2.

We now see that our operation passes to an associative operation on the set of equivalence classes of braids, since we see intuitively that we can shift z-coordinates to get from $(B_1B_2)B_3$ to $B_1(B_2B_3)$ using a homotopy between the identity map on $[0,1]$ to the map linearly projecting the intervals $[0,1/4]$, $[1/4,1/2]$ and $[1/2,1]$ onto the intervals $[0,1/2]$, $[1/2,3/4]$, and $[3/4,1]$, respectively.

We examine the braid E with purely vertical threads. This gives a unit for our operation on equivalence classes, since given a braid B we can examine both EB and BE and see that they are isotopic to B via stretching the piece looking like B and contracting the vertical threads to a point.

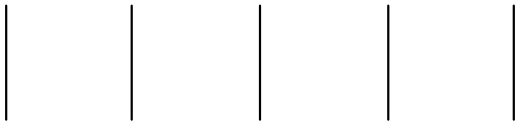


FIGURE 3. The trivial braid

An inverse for this operation then gives us a way to untangle a given braid into such vertical lines. We claim that this is given by taking the threads of a given braid and reflecting them across the plane $z = 1/2$.

2. Braid Diagrams

We now note that our current definition of a braid contains a lot more data than we really need. To deal with braids algebraically we wish to find a nice representation for each equivalence class.

We say that a **braid diagram** is given by projecting a braid onto a plane containing the z-axis, such that the following conditions hold:

(1) No three threads cross at a single point.
(2) At any point of intersection, the two intersecting threads are not tangent to one another (in other words, the intersections are **transverse**).
(3) No two crossing points have the same z-coordinate.

We claim that all braids can be expressed in such a form, so that by restricting our attention to such diagrams we do not lose anything.

DEFINITION 5.3. An **elementary braid** will be the braid diagram with $n-2$ vertical threads, as well as two diagonal threads connecting $(i, 0)$ to $(i+1, 1)$ and $(i+1, 0)$ to $(i, 1)$. Of course there are two ways for these to cross: if the former crosses over the latter we have the

FIGURE 4. Elementary braids: b_4^+ and b_3^-

elementary braid b_i^+ and if the former crosses under the latter we have the braid b_i^-.

We now see that our conditions on braid diagrams allow us to express all braids as products of elementary braids, through some isotopy of braid diagrams, meaning a homotopy from one braid diagram to another going through valid diagrams at each time. We note that two diagrams might not be isotopic as diagrams, even if they represent two

isotopic braids. This occurs since the braid isotopy would at some time violate one of our three conditions for a good diagram. Such equivalences would give relations between our generators $b_i^{\pm}$.

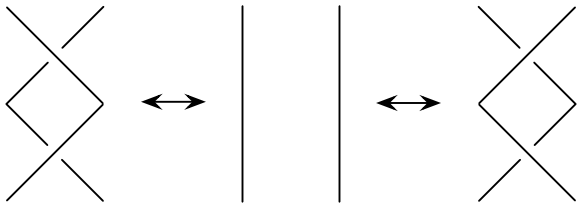


FIGURE 5. The relation $b_i^+ b_i^- = 1 = b_i^- b_i^+$

The most obvious such relation these is that b_i^+ is inverse to b_i^- for all i. When imagining the isotopy leading to the equivalence $b_i^+ b_i^- \cong 1$, we see that it will pass through a diagram violating condition (2) above.

After noting this fact, we see how the other conditions might correspond to relations. An examination of a triple crossing violating (1) will intuitively give the equivalence between $b_i^- b_{i+1}^- b_i^-$ and $b_{i+1}^+ b_i^+ b_{i+1}^+$. Likewise, an examination of a double crossing violating (3) at the same z-coordinate shows that $b_i^{\pm}$ commutes with $b_j^{\pm}$ whenever i, j are not consecutive.

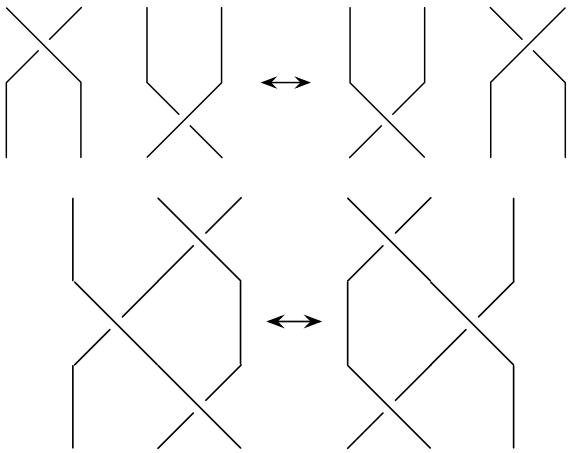


FIGURE 6. Further relations: $b_i^- b_{i+1}^- b_i^- = b_{i+1}^+ b_i^+ b_{i+1}^+$ and $b_i^{\pm} b_j^{\pm} = b_j^{\pm} b_i^{\pm}$ for $|i - j| > 1$

DEFINITION 5.4. The **braid group** Br_n is given by generators b_i as i ranges from 1 to $n - 1$, and relations of the form:

- $b_i b_{i+1} b_i = b_{i+1} b_i b_{i+1}$
- $b_i b_j = b_j b_i$ whenever $|i - j| > 1$

We see that Br_n is infinite for all n, since the generators b_i are all of infinite order. For $n > 2$ we see that Br_n is noncommutative as well. There is an obvious map into the symmetric group $Br_n \to S_n$ given by $b_i \mapsto \sigma_i$, where σ_i is the transposition switching the i-th and the $i+1$-st elements.

Definition 5.5. A **pure braid** is a braid in the kernel of this given map. In other words, pure braids are those whose threads begin at $(k, 0, 0)$ and end at $(k, 0, 1)$, thus inducing a trivial permutation of the endpoints.

3. Appearances of the Braid Group

Example 5.6. We see that Br_n is the fundamental group of the configuration space of n distinct, unordered points in the plane.

Example 5.7. We let V be a vector space, and then we can define an action of Br_n on the n-fold tensor product $V^{\otimes n} = V \otimes V \otimes \cdots \otimes V$. Here the element b_i is defined on basis elements by:

$$b_i(x_1 \otimes \cdots x_i \otimes x_{i+1} \cdots \otimes x_1) = \lambda(x_1 \otimes \cdots x_i \otimes x_{i+1} \cdots \otimes x_1)$$

Here $\lambda \neq \pm 1$ is some fixed constant in our field. We see that this action is the composition of the transposition σ_i given by the usual action of the symmetric group S_n on $V^{\otimes n}$ followed by scaling by λ. Our condition $\lambda \neq \pm 1$ guarantees that this action does not factor through the symmetric group, in other words there exist pure braids acting nontrivially (such as b_i^2). However, in general we see that there may still be nontrivial braids acting trivially.

LECTURE 6

Thursday, July 9

(These notes were written in 2009 by Claire Tomesch, with images drawn in OmniGraffle.)

1. Tangles

An anecdote survives from when the wireless telegram was invented the early twentieth century which goes as follows: a lady asked a scientist how the wireless telegram worked, to which she was told: "Visualize a cat with its head in London and its tail in Paris. When the tail is pulled in Paris, its head meows in London. The wireless telegram is like that except without the cat." This analogy applies to our current situation: considering tangles after initially playing with braids.

A misleadingly short way to describe tangles it to say that tangles are braids without the condition that the z-component of the thread functions be increasing. As an example, consider

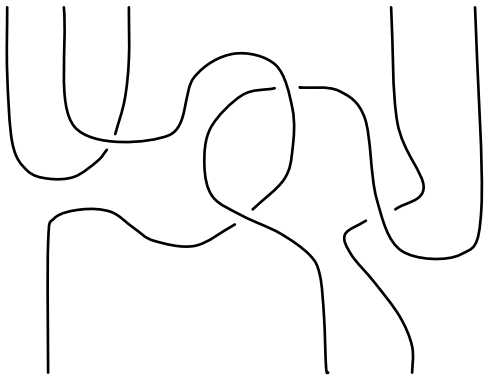


FIGURE 1. An example of a $(5, 3)$-tangle.

However, as one can see by the above example, when we eliminate this condition, we introduce many more complications – for example, that tangles are allowed to have threads that begin and end on the same surface and to have different number of intersections in the two planes of a horizontal slicing.

We want to classify such figures in a manner analogous to the method by which we classified braids; however, we run into a few problems. The method of horizontal slicing which we used before to isolate the elementary braid generators gives us "too many" tangle generators – meaning, we obtain many copies of generators which are the same up to isotopy. After some thought, we realize that we can get around this problem by keeping track of maxima and minima when making the horizontal slicings.

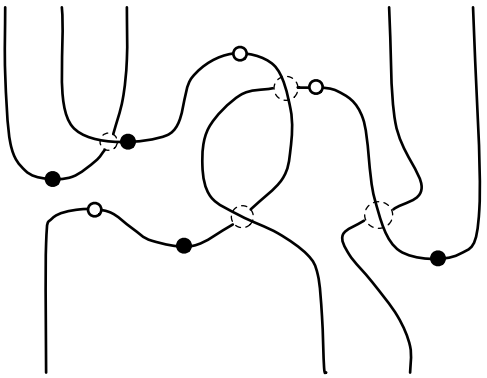


FIGURE 2. The above example with crossings, maxima, and minima marked.

DEFINITION 6.1. An (n, m)**-tangle** is a collection of $\frac{m+n}{2}+j$ disjoint maps $[0, 1] \to \mathbb{R}^3$ called **threads**, $\frac{m+n}{2}$ of which are required to take 0 to the set $\{(k, 0, 0) : k = 1, \ldots, n\}$ and 1 to $\{(k, 0, 1) : k = 1, \ldots, m\}$. Each of the other j maps are required to take 0 and 1 into the same point, which must not lie in either of the planes $z = 0$ or $z = 1$.

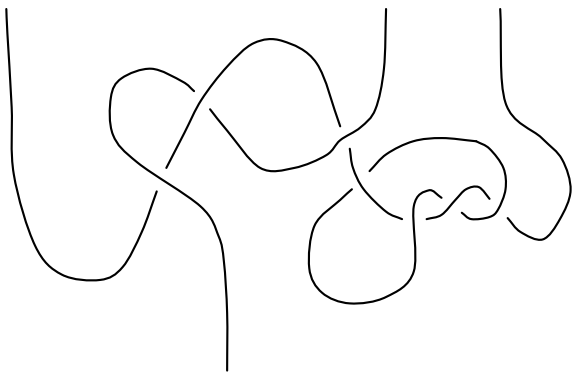


FIGURE 3. An example of an $(3, 1)$-tangle with 3 threads.

The only required relation between the integers m and n is that $m \mod 2 \equiv n \mod 2$. Given our experience with braids, we anticipate that we wouldn't be able to form a nice algebraic structure out of tangles directly, without considering them up to some notion of equivalence. Again, we have a notion of isotopy of tangles.

DEFINITION 6.2. Two tangles T_1 and T_2 are **isotopic** if there exists a map $\{[0,1] \sqcup \cdots \sqcup [0,1]\} \times [t_1, t_2] \to \mathbb{R}^3$ such that the map given by restriction to the subspace $\{[0,1] \sqcup \cdots \sqcup [0,1]\} \times \{t\}$ is a tangle for each $t \in [t_1, t_2]$, such that T_1 is the braid at time t_1 and T_2 is the tangle at time t_2.

2. Tangle Diagrams

As in the case of braids, the definition of a tangle we gave actually contains a lot more data than we really need. To deal with tangles algebraically, we want to find a nice representation for each equivalence class.

We say that a **tangle diagram** is given by projecting a tangle onto a plane containing the z-axis, such that the following conditions hold:

(1) No three threads cross at a single point.
(2) At any point of intersection, the two intersecting threads are not tangent to one another (in other words, the intersections are **transverse**).
(3) All crossings, maxima, and minima have distinct z-coordinates.
(4) No inflection points with horizontal tangent.

We claim that all tangles can be expressed in such a form, so that by restricting our attention to such diagrams we retain all the desired data.

DEFINITION 6.3. An **elementary tangle** consists of one of the following shapes with any number of vertical line segments placed to the left or right:

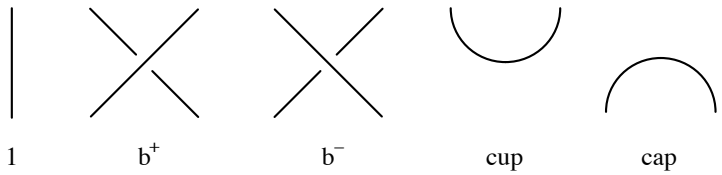
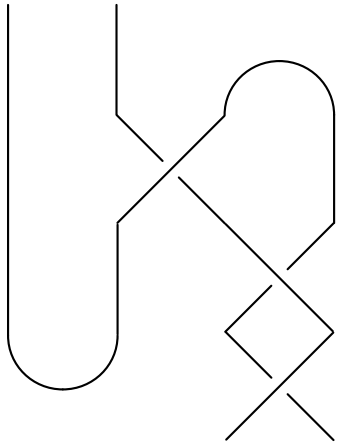


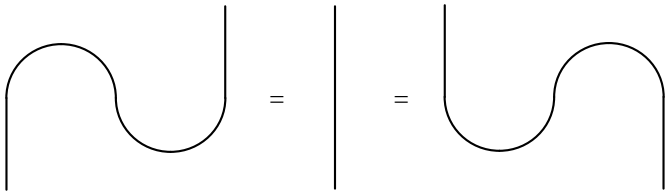
FIGURE 4. The elementary tangles, and their notations, from left to right: the trivial $(1,1)$-tangle, the two braid generators, the cup, and the cap.

One can show that all isotopy classes of tangles can be written in terms of elementary tangles, analogous to the way that we wrote all braids in terms of the elementary braids. However, when considering tangles, the most convenient way of writing them requires a bit more notation than with braids. When we isolated the braid generators, we fixed some n and then wrote them in terms of which two of the n strands were twisted and in which direction. Since for arbitrary pair of integers m, n, the collection of isotopy classes of (m, n)-tangles aren't closed under composition, it makes sense to isolate the most elementary components of tangles, independent of m and n. The notation we thus use for tangles reflects this: juxtaposition of elementary tangles is denoted by the tensor symbol, $\otimes$, while composition is denoted by juxtaposition of parenthesized groups. As an example, consider the following tangle:



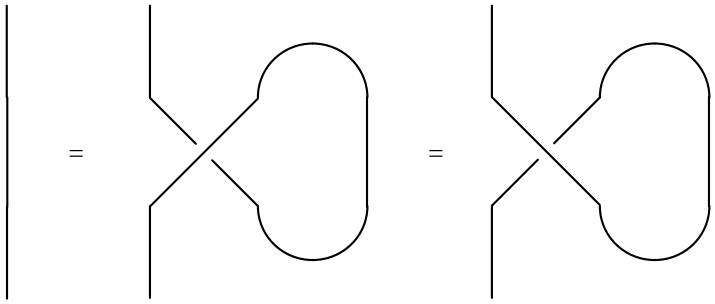
$$(1 \otimes 1 \otimes \mathit{cap})(1 \otimes b^+ \otimes 1)(1 \otimes 1 \otimes b^-)(\mathit{cup} \otimes b^+)$$

So, now that we have the tangle generators, what are the relations among them?



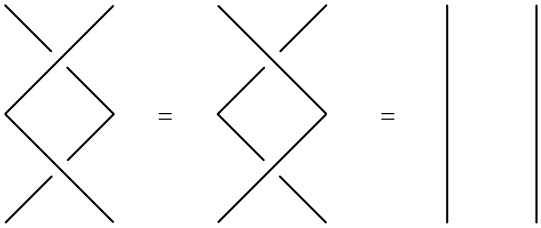
$$cap \otimes cup = 1 = cup \otimes cap$$

FIGURE 5. The "zig-zag" identity.



$$1 = (1 \otimes cap)(b^+ \otimes 1)(1 \otimes cup) = (1 \otimes cap)(b^- \otimes 1)(1 \otimes cup)$$

FIGURE 6. The first Reidemeister move.

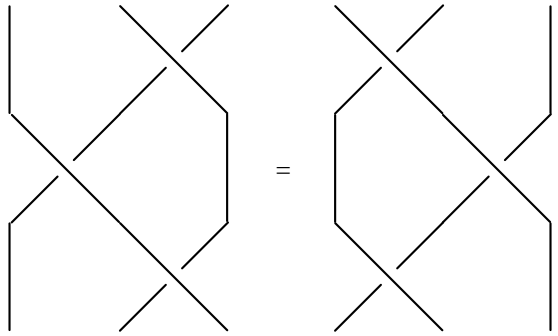


$$b^+b^- = b^-b^+ = 1 \otimes 1$$

FIGURE 7. The second Reidemeister move.

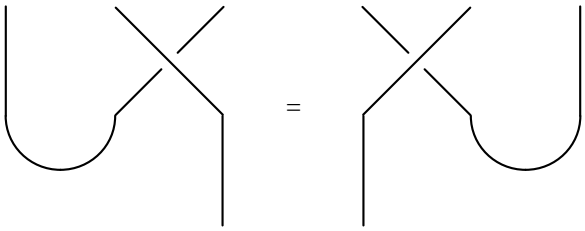
3. Bicategory of Tangles

In contrast to the case of braids, we cannot compose two (m, n)-tangles. In order to be able to compose an (m, n)-tangle with a (p, q)-tangle, we must have $n = p$ and we obtain an (m, q)-tangle as a result. Thus, even on isotopy classes of tangles, we don't have a fully defined composition; as a result, tangles don't form a group(oid). However, we can form a category involving tangles.

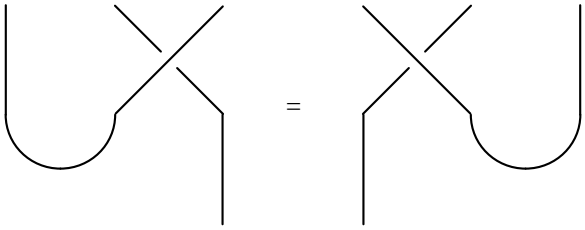


$$(1 \otimes b^-)(b^- \otimes 1)(b^- \otimes 1) = (b^- \otimes 1)(1 \otimes b^-)(b^- \otimes 1)$$

FIGURE 8. The third Reidemeister move (also called the Yang-Baxter move).



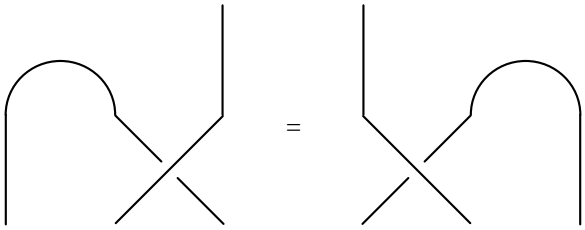
$$(1 \otimes b^-)(cup \otimes 1) = (b^+ \otimes 1)(1 \otimes cup)$$



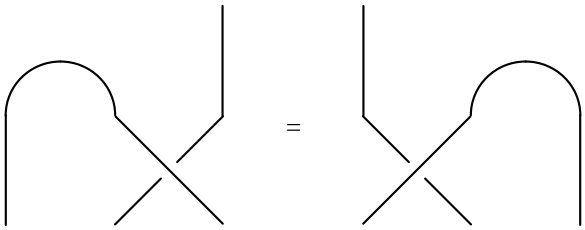
$$(1 \otimes b^+)(cup \otimes 1) = (b^- \otimes 1)(1 \otimes cup)$$

DEFINITION 6.4. The **tangle category** is the category with

(1) objects the natural numbers, $\mathbb{N}$, and
(2) a morphism between m and n is an isotopy class of (m, n)-tangles.



$$(cap \otimes 1)(1 \otimes b^+) = (1 \otimes cap)(b^- \otimes 1)$$



$$(cap \otimes 1)(1 \otimes b^-) = (1 \otimes cap)(b^+ \otimes 1)$$

By what we have just discussed, we can see that we have identity morphisms (the trivial (n, n)-tangle) and that composition is associative, so that this does indeed define a category. But there is actually more structure we can capture here than just a category. We can in fact form a **bicategory** (which we shall not discuss in detail) given by

DEFINITION 6.5. The **tangle bicategory** is the bicategory with

(1) objects the natural numbers, $\mathbb{N}$,
(2) a morphism between m and n is an isotopy class of (m, n)-tangles, and
(3) a two-cell is a isotopy of tangles, up to isotopy.

An example of a nontrivial two-cell in this bicategory is:

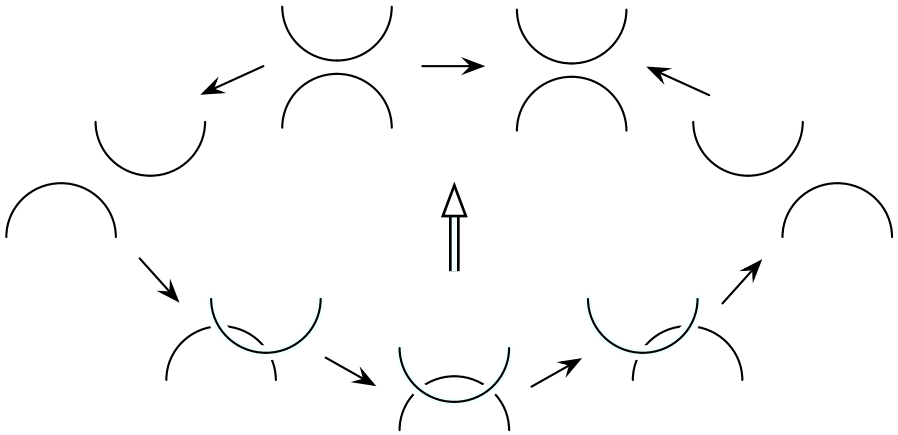


FIGURE 9. An example of a nontrivial two-cell from a nontrivial sequence of isotopies of tangles to the identity on the original $(2, 2)$-tangle.

LECTURE 7

Monday, July 13

(These notes were written in 2009 by Rolf Hoyer, based in part on notes taken in 2006 by Jim Fowler)

1. Recap: The Burnside ring and idempotents

This week we are headed towards a proof of the equivalence of the Feit-Thompson theorem to a statement about the Burnside ring $A(G)$.

We recall that a finite group G is **solvable** if there is a descending sereis of subgroups $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{e\}$ with each quotient G_i/G_{i+1} cyclic of prime order. Then the Feit-Thompson theorem states that every finite group of odd order is solvable. This deep result is the crucial starting point for the classification of simple groups.

We also recall our construction of the Burnside ring $A(G)$. Here we took isomorphism classes of finite G-sets S, and formed a rig under the operations of disjoint union and Cartesian product. Then $A(G)$ is given by formally adjoining negatives.

We have already seen that as an abelian group $A(G)$ is free on generators of the form G/H, where H ranges across the conjugacy classes of subgroups of G. The action of G on G/H is given by $k(gH) = (kg)H$, and we now note that this action is **transitive**, meaning that for any two elements of G/H there is a group element taking the first to the second.

Finally, we recall that in any ring R an element e is said to be **idempotent** if $e^2 = e$. The following transforms the statement of Feit-Thompson into a result about the Burnside ring:

THEOREM 7.1. *Given a finite group G, the only idempotents in $A(G)$ are 0 and 1 if and only if G is solvable.*

2. Commutative Algebra

On first glance there seems to be no obvious correspondence between idempotents in this constructed ring $A(G)$ and solvability of our group G. To relate these concepts we must first develop some basic theory. Throughout we will assume R to be a commutative ring.

DEFINITION 7.2. An **ideal** is a subset $I \subset R$ such that:

- I is closed under addition, meaning that if a and b are elements of I then $a + b \subset I$ as well.
- I is closed under scalar multiplication by R, meaning that if $a \in I, r \in R$, then we have $ra \in I$.

DEFINITION 7.3. A ring R is **Noetherian** if it satisfies the ascending chain condition on ideals. This means that if $I_0 \subset I_1 \subset I_2 \subset \cdots$ is an ascending chain of ideals, then $I_n = I_{n+1}$ for all sufficiently large n.

PROPOSITION 7.4. *The following three criteria are equivalent, and thus they all determine whether or not a ring R is Noetherian:*

- *R satisfies the ascending chain condition on ideals.*
- *Every nonempty set of ideals of R has a maximal element.*
- *Every ideal of R is finitely generated.*

EXAMPLE 7.5. The ring $\mathbb{Z}$ is Noetherian. All of its ideals are **principal**, meaning that that are generated by a single element, thus of the form $(n) = \{mn : m \in \mathbb{Z}\}$.

EXAMPLE 7.6. The polynomial ring $R[X_i | i \in \mathbb{N}]$ in infinitely many variables is not Notherian, because

$$(X_0), (X_0, X_1), (X_0, X_1, X_2), \cdots$$

gives an infinite ascending chain of ideals I_i with $I_i \neq I_{i+1}$.

REMARK 7.7. We recall that an R-module M is an abelian group equipped with a bilinear map $R \times M \to M$, called the action of R on M, such that $r(sm) = (rs)m$ and $1m = m$ for all r and s in R and all $m \in M$. The above proposition then holds when we replace rings and ideals with$R$-modules and R-submodules. This gives us the definition of a Noetherian module. The ascending chain condition formulation then immediately shows that any submodule of a Noetherian module is again Noetherian.

We now proceed to demonstrate how to construct new Noetherian rings out of existing ones:

THEOREM 7.8 (Hilbert Basis Theorem). *If the ring R is Noetherian, then $R[x]$ is Noetherian.*

PROOF. See Atiyah-Macdonald, p. 81. □

PROPOSITION 7.9. *If R is Noetherian and $I \subset R$ is an ideal, then R/I is Noetherian.*

PROOF. The preimage of any ideal $J \subset R/I$ under the quotient homomorphism $\pi : R \to R/I$ is an ideal J' of R. Then, J' will be finitely generated, and its generators will map under π to a finite generating set for J, as desired. □

COROLLARY 7.10. *Given a finite group G, the Burnside ring $A(G)$ is Noetherian.*

PROOF. We know that $A(G)$ is additively generated by elements corresponding to G/H_i, as H_i varies across the conjugacy classes of subgroups $H \leq G$. Let n be the number of conjugacy classes, we and construct a ring morphism $\phi : \mathbb{Z}[X_1, \dots X_n] \to A(G)$ given by $X_i \mapsto [G/H_i]$. This map is surjective, and thus $A(G)$ is isomorphic to $\mathbb{Z}[X_1, \dots X_n]/\ker\phi$, which is Noetherian. □

DEFINITION 7.11. A proper ideal P in a ring R is **prime** if $xy \in P$ implies $x \in P$ or $y \in P$.

We note as a matter of convention that R itself is never prime when considered as an ideal of itself. The trivial ideal (0) may or may not be prime, depending on whether or not R has zero-divisors.

REMARK 7.12. Why are prime ideals important? In general rings, irreducible elements might not be prime, and therefore factorizations need not be unique. For example , in $\mathbb{Z}[\sqrt{-5}]$, we have

$$2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

Nonetheless, in this case there is still unique factorization of arbitrary ideals into prime *ideals*. This is the case for a general class of examples known as **number rings**, which sit within some field analogous to the inclusion $\mathbb{Z} \subset \mathbb{Q}$. This fact explains how ideals first came to be studied, their name derives from the construction of "ideal numbers" to get around the failure of unique factorization.

DEFINITION 7.13. The spectrum of a ring $\operatorname{Spec} R$, is the collection of all prime ideals.

3. Topological Spaces

Our definition of $\operatorname{Spec} R$ does not seem immediately useful—but, surprisingly, $\operatorname{Spec} R$ is more than a set: we will see that it is also a topological space.

DEFINITION 7.14. A **topological space** is a set X with a collection $\mathcal{U}$ of subsets of X. The sets in $\mathcal{U}$ are called the **open sets** of X, and must satisfy the following properties:

- The empty set $\varnothing$ and the whole space X are open sets, i.e., $\varnothing, X \in \mathcal{U}$.
- If $U_1, \ldots, U_n \in \mathcal{U}$, then $\bigcap_{i=1}^n U_i \in \mathcal{U}$.
- If $\{U_i\}_{i \in I}$ is any subset of $\mathcal{U}$, then $\bigcup_{i \in I} U_i \in \mathcal{U}$.

The complement of an open set is an **closed set**. We call $\mathcal{U}$ a **topology** on the set X.

REMARK 7.15. A set might be open, closed, both open and closed, or neither open nor closed. We could have equivalently defined a topology as the collection of closed sets, instead requiring our collections to have finite unions and arbitrary intersections.

EXAMPLE 7.16. The usual topology given on Euclidean space $\mathbb{R}^n$ is given by arbitrary unions of finite intersections of balls of the form $B_\epsilon(x) = \{y : d(x, y) < \epsilon\}$.

We see that this example tells us how to construct a topology on any metric space (i.e., a set with a distance function). Such well-behaved examples provide us with plenty of geometric intuition. That intuition goes completely out the window for $\operatorname{Spec} R$, as we shall demonstrate.

DEFINITION 7.17. A topological space X is **Hausdorff** if for distinct points $u, v \in X$ there exist open sets $U \ni u$ and $V \ni v$ with $U \cap V = \varnothing$.

It is obvious that any metric space will be Hausdorff, corresponding to the intuitive notion that we have disjoint open balls separating any two points. However, the space $\operatorname{Spec} R$ is very far from being Hausdorff. For example, in the case $R = \mathbb{Z}$ the prime ideals are 0 and (p) for prime numbers p. We will see that the nonempty open sets are the subsets containing all but finitely many non-zero primes. Thus, any two nontrivial open sets cannot be disjoint.

LECTURE 8

Tuesday, July 14

(These notes were written in 2009 by Rolf Hoyer, based in part on notes taken in 2006 by Jim Fowler)

1. The Zariski Topology

We start with a pair of methods of constructing new ideals from already-existing ones.

DEFINITION 8.1 (Product of ideals). Let $\{I_1, \ldots, I_n\}$ be a finite set of ideals. The product $I_1 \cdots I_n$ is the ideal whose elements are all finite sums of products $x_1 \cdots x_n$ with $x_i \in I_i$.

DEFINITION 8.2 (Sum of ideals). Let $\{I_i\}_{i \in I}$ be an arbitrary set of ideals. Then $\sum_i I_i$ is the ideal whose elements are all sums $\sum_i x_i$ with $x_i \in I_i$ and all but finitely many of the x_i equal to zero.

We now define a topology $\mathcal{U}$ on the set $\operatorname{Spec} R$. For I an ideal in R, define $V(I)$ to be the prime ideals containing I, i.e.,

$$V(I) = \{P \text{ a prime ideal in } R | P \supset I\}.$$

The V stands for "variety."

Set $\mathcal{U} = \{\operatorname{Spec} R - V(I) | I \text{ an ideal in } R\}$. We check that $\mathcal{U}$ gives a topology.

- Since $V(R) = \varnothing$, we have $\operatorname{Spec} R - V(R) = \operatorname{Spec} R \in \mathcal{U}$.
- Since $V(0) = \operatorname{Spec} R$, we have $\operatorname{Spec} R - V(0) = \varnothing \in \mathcal{U}$.
- Suppose $U_1, \ldots U_n \in \mathcal{U}$, with $U_i = \operatorname{Spec} R - V(I_i)$ for an ideal I_i. We claim that

  $$V(I_1) \cup \cdots \cup V(I_n) = V(I_1 \cdots I_n).$$

  One of these inclusions is obvious, and for the other, we see that if P is prime and $P \supset I_1 \cdots I_n$, then $P \subset I_i$ for some i, otherwise we could construct an element $x_1 x_2 \cdots x_n \in I_1 \cdots I_n \subset P$ with each $x_i \in I_i, x_i \notin P$, contradicting the fact that P is prime. Taking complements in the above equality then shows:

  $$\bigcap_{i=1}^{n} U_i = \operatorname{Spec} R - V(I_1 \cdots I_n) \in \mathcal{U}.$$

- Let $\{U_i\}_{i\in I}$ be an arbitrary collection of open sets, with $U_i = \operatorname{Spec} R - V(I_i)$. Then we have the elementary relation

$$\bigcap_i V(I_i) = V\left(\sum_i I_i\right).$$

Taking complements,

$$\begin{aligned}\bigcup_i U_i &= \bigcup_i (\operatorname{Spec} R - V(I_i)) \\ &= \operatorname{Spec} R - \bigcap_i V(I_i) \\ &= \operatorname{Spec} R - V\left(\sum_i I_i\right) \in \mathcal{U},\end{aligned}$$

so the union of an arbitrary collection of open sets is in $\mathcal{U}$.

Thus, we have proven that our set $\mathcal{U}$ forms a topology, known as the **Zariski topology**, on $\operatorname{Spec} R$.

We noted that $V(0) = \operatorname{Spec} R$, and ask ourselves if there are any other ideals $I \subset R$ such that $V(I) = R$. We see that such an I will satisfy $I \subset P$ for all $P \in \operatorname{Spec} R$, and then have the following result:

PROPOSITION 8.3. *Let R be Noetherian. Then*

$$\bigcap_{P\in\operatorname{Spec} R} P = \operatorname{Nil}(R) \equiv \{x : \exists n \geq 1 \text{ such that } x^n = 0\}.$$

PROOF. First, the inclusion $\supset$ is clear, since $0 \in P$ for all ideals P, and $x^n \in P$ and P prime imply $x \in P$.

For the inclusion $\subset$, we let x be some non-nilpotent element. We let $\mathcal{I}$ be the set of ideals $I \subset R$ such that $x^n \notin I$ for all n. We let P be a maximal element in $\mathcal{I}$, which exists since R is Noetherian.

Our claim is now that P is prime. If we have $y, z \notin P$, we must show that $yz \notin P$. Since (P, y), the ideal generated by P and y strictly contains P, it does not lie in $\mathcal{I}$, and thus contains an element of the form x^m. Likewise, (P, z) contains an element of the form x^n. Then we see that $x^{m+n} \in (P, y)(P, z) \subset (P, yz)$. This shows that the latter ideal does not lie in $\mathcal{I}$, and thus from $(P, yz) \neq P$ we can conclude $yz \notin P$, as desired. □

2. Components of $\operatorname{Spec} R$

DEFINITION 8.4. A **component** of a topological space X is a subset $U \subset X$ such that U is both open and closed, and U contains no proper

subsets that are both open and closed. The set of components of a space X is denoted $\pi_0(X)$.

In order for us to understand the connection between idempotents of $A(G)$ and solvability of G, we need the following relation between idemopotents of a ring R and components of Spec R:

THEOREM 8.5. *For any fixed $n \geq 2$, there is a bijection between the following sets:*

1. *Sets $\{e_1, \ldots, e_n\}$ of nontrivial* ***orthogonal idempotents****, i.e. $e_i^2 = e_i$ and $e_i e_j = 0$ for $i \neq j$, such that we additionally have that $1 = e_1 + \ldots + e_n$.*
2. *Decompositions $R = I_1 \oplus \cdots \oplus I_n$ for nonzero ideals I_i.*
3. *Decompositions $\operatorname{Spec} R = V_1 \coprod \cdots \coprod V_n$ into with each V_i open, closed, and nonempty.*

At first glance, this result is far from obvious, especially how to relate the last set with the first two. It is a prime example of the process of translating a problem in pure algebra to a problem in topology.

We will first prove the implications (1) $\Leftrightarrow$ (2).

If we have such a set of idempotents $\{e_1, \ldots, e_n\}$, then we set I_i to be the principal ideal $(e_i) = Re_i$. The fact that $1 = e_1 + \ldots + e_n$ shows us that $R = I_1 + \ldots + I_n$.

To see that the I_i's yield a direct sum decomposition we need to verify that $I_i \cap I_j = 0$ for any $i \neq j$. If we have $a \in I_i \cap I_j$, we write it in the forms $a = re_i = se_j$. We then have $a = re_i = re_i^2 = ae_i = se_j e_i = 0$, as desired. Thus we have shown (1) $\Rightarrow$ (2).

Next, we assume that we have $R = I_1 \oplus \cdots \oplus I_n$. We then write 1 under this decomposition as $(e_1, e_2, \ldots, e_n)$. Thus we have elements e_i such that $1 = e_1 + \ldots + e_n$ and $e_i e_j \in I_i \cap I_j = 0$. We note that the e_i are neither 0 nor 1 since $1 \notin \oplus j \neq i I_j$,the latter being a proper ideal of R. Then we see

$$e_i = e_i 1 = e_i(e_1 + \ldots + e_n) = 0 + 0 + \ldots + 0 + e_i^2 + 0 + \ldots + 0 = e_i^2,$$

and thus our elements our idempotent. Thus we see (2) $\Rightarrow$ (1).

We next intend to show that we can get condition (3) from the other two.

Starting from $R = I_1 \oplus \ldots \oplus I_n$, we take an arbitary prime ideal $P \subset R$, and see that the relation $e_i e_j = 0 \in P$ means that $e_i \in P$ or $e_j \in P$. Since i, j were arbitrary, this means that overall there is at most one e_i such that $e_i \notin P$. We set $J_i = I_1 \oplus \cdots \oplus I_{i-1} \oplus I_{i+1} \oplus \cdots \oplus I_n$. Our observation that $e_i \notin P$ for at most one value of i tells us that $J_i \subset P$ for some i, and thus the sets V_i cover all of Spec R.

EXAMPLE 8.6. The above reasoning allows us to concisely classify every prime ideal P of the product ring $\mathbb{Z}^n = \mathbb{Z} \times \cdots \times \mathbb{Z}$. We see that at most one $e_i \notin P$, and so we will be done if we can find out what the least multiple of e_i lying in P is. Call this number p (this must be a prime number p or zero if no such multiple exists), and then we have $\mathbb{Z}^{i-1} \times p\mathbb{Z} \times \mathbb{Z}^{n-i}$.

To see that the V_i are disjoint, we let $J_i \subset P$ and $J_j \subset P$. The first inclusion shows that $e_k \in P$ for all $k \neq i$, and we get $e_i \in P$ from the latter shows the same for all $k \neq j$. Thus $1 = e_1 + \ldots + e_n \in P$, so $P = R$, a contradiction.

The V_i are closed by construction, and we claim they are open from $\operatorname{Spec} R - V(J_i) = \coprod_{j \neq i} V(J_j) = V(I_i)$. If we have $J_j \subset P$ for $j \neq i$, then $e_i \in P$ and thus $P \in V(I_i)$. Conversely, if $I_i \subset P$, then $e_i \in P$. Since $1 = e_1 + \ldots + e_j \notin P$. Thus $e_j \notin P$ for some $j \neq i$ and thus $P \notin V(J_i)$.

For the final implication (3) $\Rightarrow$ (2), we use a generalized version of the methods laid out in Exercise 2.25 of Eisenbud (p. 85-86).

We take such a decomposition $V(J_1) \coprod \cdots \coprod V(J_n)$ of our space $\operatorname{Spec} R$, and choose ideals I_i so that $\operatorname{Spec}(R) - V_i = V(I_i)$. We must then demonstrate $R = I_1 \oplus \cdots \oplus I_n$. We first verify

$$V(I_1 + \ldots + I_n) = \bigcap_{i=1}^{n} V(I_i) = \varnothing,$$

which implies that $I_1 + \ldots + I_n = R$, since every ideal other than R itself is contained in some prime ideal.

DEFINITION 8.7. A **maximal ideal** is a proper ideal $M \subset R$ such that if we have an ideal $I \subset R$ strictly containing M, then $I = R$.

An argument using Zorn's lemma demonstrates that every proper ideal is contained in some maximal ideal.

EXERCISE 8.8. Demonstrate that every maximal ideal is prime. This follows from the following characterizations of prime and maximal ideals:

- $I \subset R$ is prime if and only if R/I is an integral domain ($ab = 0$ implies $a = 0$ or $b = 0$)
- $I \subset R$ is maximal if and only if R/I is a field (every element has a multiplicative inverse)

We wish to show that $I_i \cap I_j = 0$ for $i \neq j$ to finish the argument. We have $V(I_i \cap V(I_j) = V(I_i) \cup V(I_j) = \operatorname{Spec} R$. This implies by our previous proposition that $I_i \cap I_j \in \operatorname{Nil}(R)$.

To sketch the remainder of the proof, an inductive argument lets us reduce to the case $n = 2$, leaving us with the following:

EXERCISE 8.9. Assume we have ideals I_1 and I_2 of R such that $I_1 + I_2 \subset \mathrm{Nil}(R)$. Write $1 = a_1 + a_2$ with $a_i \in I_i$. Then $(a_1 a_2)^q = 0$ for some q. By expanding out $1 = (a_1 + a_2)^q$, show that we have elements $e_i \in I_i$ such that $e_1 + e_2 = 1, e_1 e_2 = 0$.

LECTURE 9

Wednesday, July 15

(These notes were written in 2009 by Rolf Hoyer based in part on notes taken in 2006 by Jim Fowler

1. Orbits

Before we further examine the structure of the Burnside ring $A(G)$, we must first further examine the structure of orbits G/H. We see that if we take a conjugate gHg^{-1} we have an isomorphism of G-sets $G/H \cong G/gHg^{-1}$.

In general, we let H and K be subsets of G, and assume that we have a map of G-sets $f : G/H \to G/K$. Such maps satisfy $f(gH) = g(fH)$, and so are uniquely determined by where they send the identity coset H, so we choose $j \in G$ such that $f(H) = jK$. For our map to be well defined, we will require

$$jH = f(eH) = f(hH) = hjH$$

This implies that $j^{-1}hj \in K$, and thus we have $j^{-1}Hj \subset K$.

Definition 9.1. Let H, K be subgroups of G. Then H is **subconjugate** to K, written $(H) \leq (K)$, if there exists $g \in G$ such that $g^{-1}Hg \subset K$.

We see that this gives a partial ordering on the set of conjugacy classes of subgroups of our fixed group G such $(H) \leq (K)$ if and only if there is a map of G-sets $G/H \to G/K$.

In particular, we can examine the case $H = K$. Then our possible values of j the values of the set $N_G(H) = \{j : j^{-1}Hj = H\}$, which we will call the **normalizer** of H in G. We now note that two choices of j will yield the same map if and only if they are in the same coset of H. Thus, we get a group isomorphism $\mathrm{Aut}(G/H) \cong N_G(H)/H$. This latter group we will denote WH.

2. The ring $C(G)$

We construct a new ring $C(G) = \prod_{(H)} \mathbb{Z}_H$, where (H) ranges across the conjugacy classes of subgroups of H. We use $\mathbb{Z}_H$ to refer to a copy

of $\mathbb{Z}$ corresponding to the indexing subgroup H. The multiplication and addition in this product of rings are given coordinatewise.

REMARK 9.2. The value of this ring $C(G)$ is that unlike the Burnside ring $A(G)$, its prime ideals are very easy to understand. In fact, last time we proved that elements of $\operatorname{Spec} C(G)$ are of the form $\mathbb{Z}_K/p\mathbb{Z}_k \times \prod_{(H)\neq(K)} \mathbb{Z}_H$.

To study $A(G)$ in terms of $C(G)$, we construct a homomorphism $\chi : A(G) \to C(G)$. Such maps are uniquely determined by their coordinate projections $\chi_H : A(G) \to \mathbb{Z}_H$.

To construct such a map, by the universal property of the Grothendieck construction it suffices to give a map of rigs from the isomorphism classes of G-sets to $\mathbb{Z}$. We let this map be given by H: $\chi_H(S) = |S^H|$, where $S^H = \{x \in S : hx = x \forall h \in H\}$ is the set of fixed points under the action of H.

We must check that this map preserves our addition and multiplication operations. For the first, we clearly have $(S \coprod T)^H = S^H \coprod T^H$, demonstrating that $\chi_H(S)+\chi_H(T) = \chi_H(S \coprod T)$. Next, we claim that $(S \times T)^H = S^H \times T^H$, giving $\chi_H(S \times T) = \chi_H(S)\chi_H(T)$.

Thus, we see that χ_H extends to a map of rings $\chi_H : A(G) \to \mathbb{Z}_H$.

PROPOSITION 9.3. *The map $\chi : A(G) \to C(G)$ is a morphism, and its image is a subgroup of finite index.*

PROOF. We see that $\operatorname{Hom}(G/H, G/K)$ are given by choices of elements j such that $j^{-1}Hj \subset K$. We see that these are precisely the representatives of $(G/K)^H$, since those are characterized by $hjK = jK$ for all $h \in H$.

In particular, we can now tell that $\chi_H(G/H) = |WH|$ and $\chi_H(G/K) = 0$ unless $(H) \leq (K)$. Thus, we will have

$$\chi(G/H) = \sum_{K \leq G} \chi_K(G/H)[K] = |WH|[H] + \sum_{(K)<(H)} a_K[K]$$

We choose an ordering $H_1, \ldots, H_n$ on the conjugacy classes of subgroups of G such that $(H_i) \leq (H_j)$ implies $i \leq j$. Then the matrix representing our map χ by a matrix will be upper triangular, with nonzero entries corresponding to $|WH|$ along the diagonal.

Formally, if we choose H maximal such that $a_H \neq 0$ for a particular nonzero element $a \in A(G)$, then we have, for some constants b_J:

$$\chi\left(\sum_{(K)} a_K[G/K]\right) = |WH|[H] + \sum_{(J)\not\geq(H)} b_J[J] \neq 0.$$

This shows that χ is a monomorphism. Seeing that the image of χ has finite index now reduces to a fact about matrices with integer coefficients acting on $\mathbb{Z}^n$. The index will be precisely the absolute value of the determinant, which in this case is $\prod_{i=1}^{n} |WH_i|$. □

3. Understanding Spec $A(G)$

We use the map $\chi : A(G) \to C(G)$ to better understand Spec $A(G)$.

Lemma 9.4. *Assume we have a map of rings $f : R \to S$, and let $Q \subset S$ be a prime ideal. Then $P = f^{-1}(Q)$ is a prime ideal of R.*

Proof. If we have $xy \in P$, then $f(x)f(y) \in Q$. Thus either $f(x)$ or $f(y)$ lies in Q so that either x or y lies in P, as desired. □

Our lemma tells us that f induces a map $f^* : \operatorname{Spec} S \to \operatorname{Spec} R$. This map behaves well with respect to inclusions, and is also continuous with respect to the Zariski topologies on spectra.

In particular, setting $f = \chi : A(G) \to C(G)$, we get a map $\chi^* : \operatorname{Spec} C(G) \to \operatorname{Spec} A(G)$.

Claim 9.5. The map χ^* is surjective.

We let $\tilde{q}(H, p)$ be the prime ideal of $C(G)$ that is the product of $\mathbb{Z}/p\mathbb{Z}$ in the H coordinate and $\mathbb{Z}$ in all other coordinates. Then we set $q(H, p)$ to be $\chi^*(\tilde{q}(H, p))$, and claim that these will represent any element of Spec $A(G)$. Here we have the concrete expression $q(H, p) = \{x : \chi_H(x) \equiv 0 \pmod{p}\}$.

For Q prime in $A(G)$, we let p be the characteristic of the field given by $A(G)/Q$. We now desire to find some H such that $Q = q(H, p)$, and this will be done by letting H be a maximal element of the set $\mathcal{H} = \{H : [G/H] \notin Q\}$. The proof that this works will be deferred until tomorrow.

We note that even though every element of Spec $A(G)$ comes from such an H, p, such expressions are not unique. The following result demonstrates this, and should give some insight into the relationship with solvability that is our ultimate goal.

Proposition 9.6. *Suppose we have subgroups H and J of G such that $H \triangleleft J$ and $J/H \cong \mathbb{Z}/p\mathbb{Z}$. Then $q(H, p) = q(J, p)$.*

Proof. We note that $S^J = (S^H)^{J/H}$. Since $J/H \approx \mathbb{Z}/p\mathbb{Z}$, any orbit of its action will be size either 1 or p. Thus, we see that $|S^H| - |S^J|$ is a multiple of p. Thus, $\chi_H(x) \equiv 0 \pmod{p}$ if and only if $\chi_J(x) \equiv 0 \pmod{p}$, which is all we need. □

LECTURE 10

Thursday, July 16

(These notes were written in 2009 by Claire Tomesch.)

1. Understanding Spec $A(G)$

We give the proof, deferred from last time, that the letting the subgroup H be the minimal element of the set $\mathcal{H} = \{H : [G/H] \notin Q\}$ and $p = \text{char}(A(G)/Q)$ allows us to write $Q = q(H, p)$. To see that this works, first observe that the chain $\mathcal{H}$ is nonempty, as $[G/G] = 1 \notin Q$, and thus has a minimal element. By minimality, such H is unique up to conjugacy. Now, consider $[G/H] \cdot x$ for some element x. We claim that we can write this as

$$[G/H] \cdot x = \chi_H(x)[G/H] + \sum_{(K)<(H)} a_K[G/K].$$

However, we need only consider the case when x is an orbit; namely, we need only consider the case when the expression $[G/H] \cdot x$ is of the form $[G/H] \cdot [G/J] = [G/H \times G/J]$. Notice that the collection of K fixed points, $(G/H \times G/J)^K$ is empty unless $(K) \leq (H)$ and $(K) \leq (J)$. Thus, when H is minimal in $\mathcal{H}$, all the summands are in Q, and hence

$$[G/H] \cdot x \equiv \chi_H(x) \cdot [G/H] \mod Q.$$

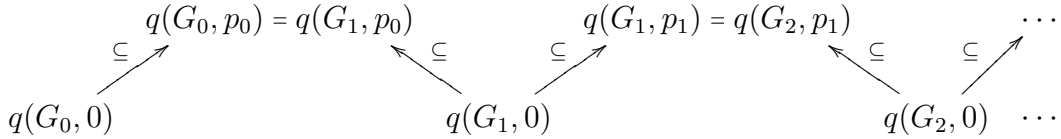
As a result, we see that $x \equiv \chi_H(x) \cdot [G/G] \mod Q$, implying that if $x \in Q$ then $\chi_H(X) \in Q$, completing the proof.

In order to proceed in our study of the structure of the prime spectrum of the Burnside ring, we need a short digression on the derived series for a group. Let $G = G_0$ be a finite group and assume G is not perfect (i.e. that $G \neq [G, G]$). Consider the abelianization of G, $Ab(G) = G/[G, G]$. By the classification of finitely generated abelian groups, $Ab(G)$ breaks up as a direct sum of finite cyclic groups. Pick some finite cyclic group $\pi_{p_0} \leq Ab(G)$ and let $G_1 := q^{-1}(\pi_{p_0})$, where q is the quotient map $q : G \to Ab(G) = G/[G, G]$. Then $G_1 \lhd G_0$. If G_1 is not perfect, then we can repeat this construction. After iterating this construction as far as possible, we obtain a chain

$$G_0 \rhd G_1 \rhd \cdots \rhd G_s$$

where $G_s = [G_s, G_s]$. We say that the group G is **solvable** if $G_s = 0$.

Now, returning to the study of $A(G)$, by previous work we know that $A(G)$ has only two kinds of prime ideals: maximal (i.e. those of the form $q(H,p)$ for $p \neq 0$) and minimal (i.e. those of the form $q(H,0)$). If we construct the derived series for G as above, we see that $q(G_i, p_i) = q(G_{i+1}, p_i)$. Then noting that $q(H,0) \subseteq q(H,p)$ for all primes p, we obtain the following graphical description of the relations among the ideals:



Since for finite sequence of closed subsets with nonempty pairwise intersection, the union lies in the same component of the space, the above diagrams tells us that all the $q(G_i, 0)$ lie in the same component of $\operatorname{Spec} A(G)$. This description gives the following result:

THEOREM 10.1. $\pi_0(\operatorname{Spec} A(G)) = \{(P) \mid P \textit{ perfect subgroup of } G\} = \{q(P,0) \mid P \textit{ perfect}\}$

2. Classification of Prime Ideals of $A(G)$

We summarize the results of our study of $\operatorname{Spec} A(G)$.

(1) All prime ideals Q of $A(G)$ are of the form $Q = q(H,p)$ for H the minimal element of $\mathcal{H} = \{H : [G/H] \notin Q\}$ and $p = \operatorname{char}(A(G)/Q)$.
(2) $q(H,0) = q(J,0)$ iff $(H) = (J)$.
(3) $q(H,p) = q(J,p)$ iff $(H_p) \sim (J_p)$, where H_p is the maximal normal subgroup of H such that H/H_p is a p-group.
(4) $q(H,0) \subseteq q(H,p)$ for all primes p.

EXERCISE 10.2. Take a small group, for example A_5, and explicitly compute all the $q(H,p)$.[1]

[1]The answer for the case of A_5 can be found in the book *Transformation Groups* by Tammo tom Dieck, 1987.