Math 901 ∼ Fall 2011 ∼ Course Notes

Information: These are class notes for the second year graduate level algebra course at UNL (Math 901) as taken in class and later typed by Kat Shultis. The notes are from the Fall of 2011, and that semester the course was taught by Brian Harbourne. During the fall semester we covered the following topics:

- Category Theory, Functors, Natural Transformations
- Group Theory: Free (Abelian) Groups, Group Actions, Semi-Direct Products, Sylow Theorems, Nilpotent Groups, Solvable Groups
- Field Theory: Algebraic Extensions, Separable Extensions, Separable Degree, Galois Theory, Galois Extensions, Finite Fields, Transcendence Degree, Transcendence Bases

For each class day, I’ve indicated the topic at the top of that day’s notes.

Disclaimer: I created these notes in order to help me study, and so I’ve expanded proofs where I find it useful, shortened things I was comfortable with before this course, and changed at least one proof to one that I like better than the one presented in class. These notes are not meant to be a substitute for your own notes. They have been proof-read, but are not guaranteed to be without errors. If you find errors, please email Kat at the following address: s-kshult11 “at” math.unl.edu

22 August 2011

- Comment: The purpose of categories and functors is to describe structure that is common in many parts of mathematics.
- Comment: Intuitively, a category is a structure consisting of objects and arrows (morphisms), and the arrows are maps between the objects.
- Examples:

<table>
<thead>
<tr>
<th>Category</th>
<th>Objects</th>
<th>Arrows</th>
<th>Typical Notation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets</td>
<td>sets</td>
<td>set maps</td>
<td>S</td>
</tr>
<tr>
<td>Groups</td>
<td>groups</td>
<td>group homomorphisms</td>
<td>G</td>
</tr>
<tr>
<td>Abelian Groups</td>
<td>abelian groups</td>
<td>group homomorphisms</td>
<td>Ab</td>
</tr>
<tr>
<td>Rings</td>
<td>rings</td>
<td>ring homomorphisms</td>
<td></td>
</tr>
<tr>
<td>Vector Spaces</td>
<td>finite dimensional R-vector spaces</td>
<td>linear transformations</td>
<td>V</td>
</tr>
<tr>
<td>Manifolds</td>
<td>topological manifolds</td>
<td>continuous maps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>differentiable manifolds</td>
<td>differentiable maps</td>
<td></td>
</tr>
<tr>
<td>Group, G</td>
<td>*</td>
<td>elements of G</td>
<td></td>
</tr>
</tbody>
</table>

- Definition: A category, $\mathcal{A}$, consists of a collection of objects, $\text{Ob}(\mathcal{A})$, and for each pair of objects, $A, B \in \text{Ob}(\mathcal{A})$, there is a set of morphisms, $\text{Mor}(A, B)$, and a composition law defined for morphisms $\varphi \in \text{Mor}(A, B)$ and $\psi \in \text{Mor}(B, C)$ when $A, B, C \in \text{Ob}(\mathcal{A})$, such that $\psi \circ \varphi \in \text{Mor}(A, C)$, which satisfies the following:

1. Composition is associative when defined.
2. For all $A \in \text{Ob}(\mathcal{A})$, there exists a unique identity morphism, which is a left and right identity whenever composition is defined. That is, there is a morphism $1_A \in \text{Mor}(A, A)$ such that if $\varphi \in \text{Mor}(A, B)$ and $\psi \in \text{Mor}(B, A)$, then $\varphi \circ 1_A = \varphi$ and $1_A \circ \psi = \psi$.
3. $\text{Mor}(A, B) \cap \text{Mor}(A', B') = \emptyset$, unless $A = A'$ and $B = B'$, in which case $\text{Mor}(A, B) = \text{Mor}(A', B')$.

24 August 2011

- Example: Let $X$ be a topological space. We’ll use $T_X$ as the collection of open sets in $X$. We can turn this into a category, by setting $\text{Ob}(X) = T_X$, and if $U, V \in T_X$, we have either $\text{Mor}(U, V) = \emptyset$ when $U \nsubseteq V$ or $\text{Mor}(U, V) = \{U \subseteq V\}$ when $U \subseteq V$.

- Definition: A morphism $f : A \to B$ in a category $\mathcal{C}$ is an isomorphism if and only if there is a morphism $g : B \to A$ such that $g \circ f = id_A$ and $f \circ g = id_B$.

- Comment: We discussed the idea of direct products, and how a direct product is really just a function. This was a bit confusing, but the general idea was to generalize n-tuples. I’ll only put it here in the most general context, not in the more specific cases we discussed.

---

1 These are actually equalities and not isomorphisms. In the category of groups, for example, my copy of $\mathbb{Z}$ is isomorphic, but not necessarily equal to, Sarah’s copy of $\mathbb{Z}$, and the morphisms from my copy to Caitlyn’s copy are hence fundamentally different from the morphisms from Sarah’s copy to Caitlyn’s copy.
Definition: Let \( \{ A_i : i \in I \} \) be a family of objects in a category \( C \). We say \( P \in \text{Ob}(C) \) is a **product** of the objects \( A_i \), sometimes written \( \prod_{i \in I} A_i \), if \( P \) was given together with morphisms \( \pi_i : P \to A_i \) called projections such that they satisfy the universal property. That is, given any \( B \in \text{Ob}(C) \) and morphisms \( f_i : B \to A_i \) there is a unique morphism \( \prod_{i \in I} f_i = \varphi \in \text{Mor}(B, P) \) such that the diagram below commutes for each \( i \in I \).

\[
\begin{array}{ccc}
B & \xrightarrow{\varphi} & P \\
\downarrow{f_i} & & \downarrow{\pi_i} \\
A_i & & \\
\end{array}
\]

Aside: Suppose \( P \) and \( P' \) are both products, that is we have projections \( \pi_i : P \to A_i \) and \( \pi_i' : P' \to A_i \). Then by the universal property we have morphisms \( f : P \to P' \) and \( g : P' \to P \), and these are inverse morphisms because the diagram below commutes.

\[
\begin{array}{ccc}
P' & \xrightarrow{f} & P \\
\downarrow{\pi_i'} & & \downarrow{\pi_i} \\
A_i & \xleftarrow{\pi_i'} & \\
\end{array}
\]

In other words \( \pi_i' \circ g \circ f = \pi_i' \) and so we must have that \( g \circ f = 1_{P'} \) and similarly \( 1_P = f \circ g \). Hence \( P \) and \( P' \) are isomorphic. However, note that we can actually only use this diagram for one direction, that is we can only show that \( g \circ f = 1_{P'} \). However, a similar argument will show the other direction. Once things are more formal, we’ll see that objects satisfying universal properties are unique.²

---

26 August 2011

Review: From last time, we discussed the categorical product, and we’ve discussed the category of a topological space, \( X \). The product of \( U \) and \( V \) in this category is their intersection. For homework, we’ll ask more sophisticated questions about the product.

Example: Let \( C \) be the category whose objects are all the elements in the set \( \mathbb{R} \cap [0, 1] \), and \( \text{Mor}(x, y) = \{ \emptyset, \{ x \} \} \), if \( x > y \). Let \( \{ x_i : i \in I \} \) be a collection of objects in this category, then the categorical product is \( p = \inf\{ x_i : i \in I \} \). This is easily seen to be what you want if you do the case of two objects and their product, so that the product of \( x \) and \( y \) is \( \min(x, y) \).

Definition: Let \( C \) be a category and let \( A, B \in \text{Ob}(C) \), with \( \varphi \in \text{Mor}(A, B) \). We say \( \varphi \) is a **monomorphism** if given any \( \gamma, \delta \in \text{Mor}(C, A) \) with \( \varphi \circ \gamma = \varphi \circ \delta \) then \( \gamma = \delta \).

Proposition: In the category of sets, \( \varphi \) is a monomorphism if and only if it is injective.

Definition: (Again, using pictures) A map \( \varphi \) is a **monomorphism** if whenever we have

\[
\begin{array}{ccc}
C & \xrightarrow{\gamma} & A \\
\downarrow{\delta} & & \downarrow{\varphi} \\
& B \\
\end{array}
\]

and it commutes, then \( \gamma = \delta \).

Comment: An epimorphism is the categorical dual of a monomorphism, and also a generalization of a surjective map.

Definition: A map \( \varphi \) is an **epimorphism** if whenever we have

\[
\begin{array}{ccc}
C & \xleftarrow{\gamma} & A \\
\downarrow{\delta} & & \downarrow{\varphi} \\
& B \\
\end{array}
\]

and it commutes, then \( \gamma = \delta \).

²Also, the argument is frequently almost identical to this one.
Example: Back to the order relations. Here, all morphisms are both monomorphisms and epimorphisms, but only the identity morphisms are isomorphisms. This indicates that the mono- and epi-morphisms are related to injective and surjective maps, but do not always act the same.

Comment: The categorical dual of a product is a coproduct. Also, in most cases, categorical duals can be defined by simply reversing the directions of the arrows.

29 August 2011     Coproducts; Initial & Terminal Objects

Comment: We’ll repeat the definition of a product here, so that we can compare it to the dual, the coproduct.

Definition: Let \( \{ A_i : i \in I \} \) be a family of objects in a category \( C \).

The product (if it exists) is an object \( \prod_{i \in I} A_i \) with a family of morphisms \( \pi_j : \prod_{i \in I} A_i \to A_j \) such that given any object \( B \) and family of morphisms \( p_j : B \to A_j \), there is a unique morphism \( \varphi : B \to \prod_{i \in I} A_i \) such that the diagram below commutes for each \( j \in I \).

\[
\begin{array}{ccc}
B & \xrightarrow{\varphi} & \prod_{i \in I} A_i \\
\downarrow & & \downarrow \pi_j \\
A_j & &
\end{array}
\]

The coproduct (if it exists) is an object \( \coprod_{i \in I} A_i \) with a family of morphisms \( \tilde{\pi}_j : A_j \to \coprod_{i \in I} A_i \) such that given any object \( B \) and family of morphisms \( \tilde{p}_j : A_j \to B \), there is a unique morphism \( \varphi : \coprod_{i \in I} A_i \to B \) such that the diagram below commutes for each \( j \in I \).

\[
\begin{array}{ccc}
B & \xleftarrow{\varphi} & \coprod_{i \in I} A_i \\
\uparrow & & \uparrow \tilde{\pi}_j \\
A_j & &
\end{array}
\]

Example: The category of abelian groups. In this category, the coproduct is the direct sum.

Example: The category of sets. In this example, the coproduct is the disjoint union. Let’s make that concept a bit more rigorous: Let \( \{ A_i : i \in I \} \) be our collection of sets. Then set \( \tilde{A}_i = \{ i \} \times A_i \subseteq I \times \bigcup_{i \in I} A_i \), so that \( \tilde{A}_i \cap \tilde{A}_j = \emptyset \) if \( i \neq j \). Then \( P = \bigcup_{i \in I} \tilde{A}_i \) works and \( \tilde{\pi}_j : A_j \to P \) is given by \( x \mapsto (j, x) \).

Definition: An object, \( I \) in a category \( C \) is said to be initial (aka universally repelling) if there is a unique morphism \( I \to A \) for every object \( A \in \text{Ob}(C) \).

Definition: An object \( T \) in a category \( C \) is said to be terminal (aka universally attracting) if there is a unique morphism \( A \to T \) for every object \( A \in \text{Ob}(C) \).

Example: The initial object in the category of abelian groups is the trivial group, \( I = (0) \). In the category corresponding to a topological space, the empty set is an initial object, and the whole space is a terminal object.

Theorem: If \( A \) and \( B \) are initial (respectively terminal) objects in a category \( C \), then there is a unique isomorphism \( \varphi : A \to B \).

31 August 2011     Topology Review; (co)Products as (Initial)Terminal Objects

Comment: We discussed a variety of possible definitions of continuity, and how these arose in history. We also discussed the idea that topology was in some ways a natural abstraction of other areas of mathematics. We then proceeded to define a topology (defined using open sets), closed sets, the closure and interior, the topological definition of continuous, and a basis. We then proceeded to continue our discussion of initial and terminal objects. The purpose
of this discussion was to introduce ideas that show up in the first homework assignment due Friday. I omit the details here as I was already comfortable with these definitions.

**Definition:** Let \( \mathcal{C} \) be a category, and let \( \mathcal{F} = \{ A_i : i \in I \} \) be a family of objects in \( \mathcal{C} \). We define a new category \( \mathcal{C}_\mathcal{F} \). In this category, the objects are the objects of \( \mathcal{C} \) together with a family of morphisms \( f_i \in \text{Mor}(C, A_i) \) for each \( i \in I \). We’ll denote this object as \( C_{\{f_i\}} \). Given two objects in this category \( C_{\{f_i\}} \) and \( D_{\{g_i\}} \), a morphism \( \varphi \in \text{Mor}(C_{\{f_i\}}, D_{\{g_i\}}) \) is a morphism \( \varphi \in \text{Mor}(C, D) \) in the original category such that the diagram (existing in the category \( \mathcal{C} \)) below commutes for all \( i \in I \).

\[
\begin{array}{ccc}
C & \xrightarrow{\varphi} & D \\
\downarrow{f_i} & & \downarrow{g_i} \\
A_i & & \\
\end{array}
\]

**Comment:** The product in \( \mathcal{C} \) is precisely a terminal object in \( \mathcal{C}_\mathcal{F} \).  

**Definition:** Let \( \mathcal{C} \) be a category, and let \( \mathcal{F} = \{ A_i : i \in I \} \) be a family of objects in \( \mathcal{C} \). We define a new category \( \mathcal{C}_\mathcal{F} \). In this category, the objects are the objects of \( \mathcal{C} \) together with a family of morphisms \( f_i \in \text{Mor}(A_i, C) \) for each \( i \in I \). We’ll denote this object as \( C_{\{f_i\}} \). Given two objects in this category \( C_{\{f_i\}} \) and \( D_{\{g_i\}} \), a morphism \( \varphi \in \text{Mor}(D_{\{g_i\}}, C_{\{f_i\}}) \) is a morphism \( \varphi \in \text{Mor}(D, C) \) in the original category such that the diagram (existing in the category \( \mathcal{C} \)) below commutes for all \( i \in I \).

\[
\begin{array}{ccc}
& \xleftarrow{\varphi} & C \\
D & \downarrow{g_i} & \downarrow{f_i} \\
& A_i & \\
\end{array}
\]

**Comment:** The coproduct in \( \mathcal{C} \) is precisely an initial object in \( \mathcal{C}_\mathcal{F} \).  

---

**2 September 2011**  

**Fiber Products**  

**Comment:** For intuition, we discuss the fiber product in the category of sets. Given \( X, Y, Z \) sets with \( f : X \to Z \) and \( g : Y \to Z \) the fiber product is the product of the fibers, that is, \( X \times_Z Y = \{ f^{-1}(z) \times g^{-1}(z) : z \in Z \} \), or more traditionally though of as \( X \times_Z Y = \{ (x, y) \in X \times Y : f(x) = g(y) \} \).

**Definition:** Let \( A, B \in \text{Ob}(\mathcal{C}) \) for \( \mathcal{C} \) some category, and let \( f \in \text{Mor}(A, C) \) and \( g \in \text{Mor}(B, C) \) be morphisms. We say an object \( F \) together with morphisms \( \alpha \in \text{Mor}(F, A) \) and \( \beta \in \text{Mor}(F, B) \) is a fiber product of \( f \) and \( g \) if

- the diagram below commutes:

\[
\begin{array}{ccc}
A & \xrightarrow{f} & C \\
\downarrow{\alpha} & & \downarrow{g} \\
F & \xleftarrow{\beta} & B \\
\end{array}
\]

- and whenever we have morphisms \( \varphi \in \text{Mor}(G, A) \) and \( \psi \in \text{Mor}(G, B) \) such that the diagram below commutes

\[
\begin{array}{ccc}
& \xrightarrow{\varphi} & G \\
A & \downarrow{f} & \downarrow{g} \\
& \xleftarrow{\psi} & B \\
& C & \\
\end{array}
\]
then there is a unique morphism $\theta \in \text{Mor}(G, F)$ such that the third diagram below commutes.

![Diagram]

\[ \begin{array}{ccc} G & \xrightarrow{\theta} & F \\ \downarrow{\varphi} & & \downarrow{\psi} \\ A & \xrightarrow{\alpha} & B \\ \downarrow{f} & & \downarrow{g} \\ C & \xrightarrow{\beta} & D \end{array} \]

**Comment:** The categorical fiber product of $f \in \text{Mor}(A, C)$ and $g \in \text{Mor}(B, C)$ in a category $\mathcal{C}$ is just a categorical product of objects $A_{\{f\}}$ and $B_{\{g\}}$ in the category $\mathcal{C}_{\{C\}}$.

**Definition:** We next started to think about functors, and discussed the idea of a subcategory, but did not complete the definition of a functor.

**Definition:** We say a category $\mathcal{C}$ is a **subcategory** of a category $\mathcal{D}$ if $\text{Ob}(\mathcal{C}) \subseteq \text{Ob}(\mathcal{D})$ and if given $A, B \in \text{Ob}(\mathcal{C})$, then $\text{Mor}_\mathcal{C}(A, B) \subseteq \text{Mor}_\mathcal{D}(A, B)$ and if moreover an identity in $\mathcal{C}$ is an identity in $\mathcal{D}$, and the composition law in $\mathcal{C}$ agrees with the composition law in $\mathcal{D}$.

**Example:** The category of abelian groups is a subcategory of the category of groups. The inclusion of the category of abelian groups in the category of groups is an example of a covariant functor.

---

**7 September 2011**

**Functors**

**Definition:** Let $\mathcal{C}$, $\mathcal{D}$ be categories. A **covariant functor** $F : \mathcal{C} \to \mathcal{D}$ is an assignment of an object $F(A)$ in $\mathcal{D}$ for each object $A$ in $\mathcal{C}$, and for each morphism $\varphi : A \to B$ of objects in $\mathcal{C}$, a morphism $F(\varphi) : F(A) \to F(B)$ such that
- $F(1_A) = 1_{F(A)}$, and
- if we have morphisms $f : A \to B$ and $g : B \to C$ in $\mathcal{C}$, then $F(g \circ f) = F(g) \circ F(f)$.

A **contravariant functor** $F : \mathcal{C} \to \mathcal{D}$ is an assignment of an object $F(A)$ in $\mathcal{D}$ for each object $A$ in $\mathcal{C}$, and for each morphism $\varphi : A \to B$ of objects in $\mathcal{C}$, a morphism $F(\varphi) : F(B) \rightarrow F(A)$ such that
- $F(1_A) = 1_{F(A)}$, and
- if we have morphisms $f : A \to B$ and $g : B \to C$ in $\mathcal{C}$, then $F(g \circ f) = F(f) \circ F(g)$.

**Examples:**
- The inclusion of abelian groups into groups is a covariant functor.
- The forgetful functor is a covariant functor. For example, we could have this functor from the category of groups to the category of sets, where the functor sends a group to its underlying set and a group homomorphism is sent to itself (as a set map).

**Comment:** The next few items here are intended as a review of things necessary to understand the double dual as a covariant functor, and the dual as a contravariant functor.

**Definition:** Given a vector space $V$, the **dual** of $V$ is $V^* = \text{Mor}(V, \mathbb{R})$.

**Definition:** Given vector spaces $V, W$ and a linear map $f : V \to W$, we define the **dual** of the map as $f^* : W^* \to V^*$ via $f^*(\varphi) = \varphi \circ f$ where $\varphi : W \to \mathbb{R}$ is any linear transformation.

**Recall:** If $V$ is a real finite dimensional vector space, then $\text{Mor}(V, \mathbb{R})$ is as well; moreover, they have the same dimension, so there exists an isomorphism between $V$ and $V^{**}$ (and with $V^*$ but we care significantly less about that here).

**Definition:** Let $\mathcal{V}$ be the category whose objects are real finite dimensional vector spaces, with morphisms as linear transformations.

**Example:** We now define the functor $F : \mathcal{V} \to \mathcal{V}$ as follows. Given an object $V \in \text{Ob}(\mathcal{V})$, then $F(V) = V^{**}$. Also, if $V, W \in \text{Ob}(\mathcal{V})$, with $f \in \text{Mor}(V, W)$, then $F(f)$ is a map from $F(V)$ to $F(W)$, that is from $V^{**}$ to $W^{**}$ given by $F(f) = (f^*)^* = f^{**}$.

**Lemma:** Given $f : V \to W$ and $g : W \to Z$, where $V, W, Z$ are finite dimensional real vector spaces, and $f, g$ are linear transformations, then $(g \circ f)^* = f^* \circ g^*$.

**Proof.** Let $\varphi \in Z^*$, that is $\varphi : Z \to \mathbb{R}$. Then it is clear that $(g \circ f)^*(\varphi) = \varphi \circ (g \circ f)$. Also, we have that $(f^* \circ g^*)(\varphi) = f^*(g^*(\varphi)) = f^*(\varphi \circ g) = (\varphi \circ g) \circ f$. Now, as composition of morphisms is associative, we have that the action of $(g \circ f)^*$ and of $f^* \circ g^*$ is the same, and hence, they are the same function.

---

\(^5\)See 31 August 2011 for a reminder of what this category is.
Proposition: As defined $F : V \to V$ is a covariant functor.

Proof. First, we'll check that $F(1_V) = 1_{F(V)}$ or equivalently, that $(1_V)^* = 1_{V^*}$. So let $\varphi \in V^*$ so that $\varphi : \text{Mor}(V,R) \to R$. Then clearly, $1_{V^*}(\varphi) = \varphi$. Also, $1_{V^*}(\varphi) = \varphi \circ 1_{V^*}$. Both of these are maps from $V^*$ to $V^*$, and we want to check they are the same map. So let $\lambda \in V^*$. Then $1_{V^*}(\varphi)(\lambda) = \varphi \circ \lambda$. Also, $1_{V^*}(\varphi)(\lambda) = (\varphi \circ 1_{V^*})(\lambda) = \varphi(1_{V^*}(\lambda)) = \varphi \circ \lambda \circ 1_{V^*} = \varphi \circ \lambda$. Hence, we have $F(1_V) = 1_{F(V)}$.

Now, let $f : V \to W$, and $g : W \to Z$ where $V, W, Z \in \text{Ob}(V)$ and $f, g$ are morphisms. Then we'll check that $F(g \circ f) = F(g) \circ F(f)$. From the Lemma, we know that $(g \circ f)^* = f^* \circ g^*$. So applying the lemma to $f^* \circ g^* = (g \circ f)^*$ then gives that $F(g \circ f) = ((g \circ f)^*)^* = (f^* \circ g^*)^* = g^{**} \circ f^{**} = F(g) \circ F(f)$ as required. \qed

9 September 2011

More on Functors

Example: We can get a contravariant functor $D : V \to V$ by taking duals. On objects, the functor is defined by $D(W) = W^* = \{ \lambda : W \to R | \lambda \text{ is a linear transformation} \}$. On morphisms, $f : V \to W$, $D(f) = f^*$ known as the “pull back” morphism and is obtained by composing with $f$.\(^6\) We checked in class that this was a contravariant functor, but Sarah and I did that work already, and the explanation is already incorporated into the notes for the previous class (7 Sept 2011).

Comment: We get the covariant functor from last time by composing $D$ with itself, or equivalently, using “push forwards.” That is, we can define $F : V \to V$ by $F(W) = W^{**}$ and $F(f) = f_*$. We now describe this push forward.

Definition: Given $f : V \to W$ we want to define $f_* : V^{**} \to W^{**}$. Let $\varphi \in V^{**}$. We have a morphism, $\varphi : V^* \to R$ and we know what $f^*$ is, and so we define $f_*(\varphi) = \varphi \circ f^*$.

Alternate Viewpoint: Given $f : V \to W$ and $\varphi : V^* \to R$, we want $f_*(\varphi)$ to be an element of $W^{**}$, so we should be able to evaluate $f_*(\varphi)$ at elements $\lambda \in W^*$. We then define $(f_*(\varphi))(\lambda) = \varphi(\lambda \circ f)$.\(^7\)

Definition: Let $F$ be a covariant functor $F : C \to D$. Then for any two objects $C_1, C_2$ in $C$, there is a map $\text{Mor}(C_1, C_2) \to \text{Mor}_D(F(C_1), F(C_2))$ which is given by $f \mapsto F(f)$.

- If the map is injective for all $C_1, C_2$ in $C$, then we say $F$ is faithful.
- If the map is surjective for all $C_1, C_2$ in $C$, then we say $F$ is full.
- If the map is bijective for all $C_1, C_2$ in $C$, then we say $F$ is fully faithful.

Examples:

- The inclusion functor from the category of abelian groups to the category of groups is fully faithful.
- The forgetful functor from the category of groups to the category of sets is faithful but not full.
- The functor from the category of sets to the category with a single object, and single morphism is full, but not faithful.

12 September 2011

Functor Categories & Representability of Functors

Motivation: We discussed the motivation for functor categories. The basic idea was to stick in things that we want to have in our categories, and then maybe they were already there, but we have them now. We then defined two representation functors.

Definition: Let $A$ be a category, and let $A$ be an object in $A$. Then we define a covariant functor, $M_A$ from $A$ to the category of sets, $S$. On objects, this functor is $M_A(B) = \text{Mor}(A,B)$, and if $f \in \text{Mor}(A,C,D)$, then $M_A(f)$ should be a morphism from $\text{Mor}(A,C)$ to $\text{Mor}(A,D)$, so we set $M_A(f) = f_*$ where $f_*$ is the push forward map, $f_*(g) = f \circ g$.

Proposition: The above defines a covariant functor.\(^8\)

Definition: Similarly, we define a contravariant functor, $M^A$ from $A$ to $S$. On objects, the functor is $M^A(B) = \text{Mor}(A,B)$, and if $f \in \text{Mor}(A,C,D)$, then $M^A(f)$ should be a map from $\text{Mor}(A,D,A)$ to $\text{Mor}(A,C,A)$, so we set $M^A(f) = f^*$ where $f^*$ is the pull back map, $f^*(g) = g \circ f$.

Proposition: The above defines a contravariant functor.\(^9\)

---

\(^6\)and was also defined on 7 Sept 2011

\(^7\)I'm not sure how this helps, it may make more sense if we had other examples of a push forward, right now, it seems like a pull back still and to be honest, I'm a bit confused.

\(^8\)The proof is not difficult, but it can be confusing to think about.

\(^9\)The proof is not difficult, but it can be confusing to think about.
Definition: Let $\mathcal{C}$ and $\mathcal{D}$ be categories. Also, let $F$ and $G$ be covariant functors from $\mathcal{C}$ to $\mathcal{D}$. A natural transformation from $F$ to $G$ is a rule, $\Phi$ which assigns to every object $C$ of $\mathcal{C}$ a morphism $\Phi_C \in \text{Mor}_\mathcal{D}(F(C), G(C))$ such that given any morphism $f \in \text{Mor}(C_1, C_2)$ in $\mathcal{C}$, the diagram below commutes:

$$
\begin{array}{ccc}
F(C_1) & \xrightarrow{F(f)} & F(C_2) \\
\Phi_{C_1} & \downarrow & \Phi_{C_2} \\
G(C_1) & \xrightarrow{G(f)} & G(C_2)
\end{array}
$$

Fact: Let $\mathcal{C}$ and $\mathcal{D}$ be categories. Let $\mathcal{C}^\mathcal{D}$ be the collection of covariant functors from $\mathcal{C}$ to $\mathcal{D}$. This becomes a category if given two covariant functors $F$ and $G$ from $\mathcal{C}$ to $\mathcal{D}$ we define $\text{Mor}_{\mathcal{C}^\mathcal{D}}(F, G)$ to be the natural transformations from $F$ to $G$.

Definition: A natural equivalence is a natural transformation which is an isomorphism in the functor category.

Definition: A covariant functor, $F$, from a category $\mathcal{C}$ to the category $\mathcal{S}$ is said to be representable if $F$ is naturally equivalent to $M_A$ for some object $A$ in $\mathcal{C}$.

A contravariant functor, $G$ from $\mathcal{C}$ to the category $\mathcal{S}$ is representable if $G$ is naturally equivalent to $M^A$ for some object $A$ in $\mathcal{C}$.

Comment: We’re now ready to discuss the vector space example again. Next time, we’re going to show that the double dual functor is naturally equivalent to the identity functor on the category $\mathcal{V}$ as defined on 7 September 2011.

14 September 2011

Example: We spent all of this day explaining why the identity functor on $\mathcal{V}$, which we’ll denote $1_\mathcal{V}$, is naturally equivalent to the double dual functor, $F$ (as defined on 7 September 2011).

- Step 1: First we defined an evaluation map $e_w^W : W^* \to \mathbb{R}$ for any fixed object $W$ in $\mathcal{V}$ and any fixed element $w \in W$, by $\lambda \mapsto \lambda(w)$. We showed this is a linear map, and hence is an element of $W^{**}$.
- Step 2: We next defined a map $e^W : W \to W^{**}$ for any finite dimensional real vector space, $W$ via $w \mapsto e_w^W$. We again showed this is a linear map, and hence an object of $\text{Mor}_\mathcal{V}(W, W^{**})$.
- Step 3: We next defined a natural transformation $\Phi$ from $1_\mathcal{V}$ to $F$. For each object $W$ of $\mathcal{V}$ we need a morphism $\Phi_W : 1_\mathcal{V}(W) \to F(W)$. Note that $1_\mathcal{V}(W) = W$ and $F(W) = W^{**}$. We’ll take $\Phi_W = e^W$. We must show that this is natural. That is, given any morphism $L : W_1 \to W_2$ of real finite dimensional vector spaces, we must show that the following diagram commutes:

$$
\begin{array}{ccc}
1_\mathcal{V}(W_1) & \xrightarrow{L} & 1_\mathcal{V}(W_2) \\
e_{W_1} & \downarrow & e_{W_2} \\
F(W_1) & = & F(W_2)
\end{array}
$$

We’ll rewrite the diagram with “easier” notation:

$$
\begin{array}{ccc}
W_1 & \xrightarrow{L} & W_2 \\
e_{W_1} & \downarrow & e_{W_2} \\
W_1^{**} & = & W_2^{**}
\end{array}
$$

We checked that the diagram commutes in class, and it was not difficult.

Aside: For a natural transformation $\Phi$ to be a natural equivalence, we just need for each object $W$, that $\Phi_W$ is an isomorphism. We can then define an inverse natural transformation $\Psi$ as $\Psi_W = (\Phi_W)^{-1}$ and then we just need to check $\Psi$ is a natural transformation and that it is an inverse to $\Phi$. However, I believe Brian Harbourne said this will ALWAYS happen if each $\Phi_W$ is an isomorphism.

---

10 You can similarly define a natural transformation of contravariant functors by changing the direction of the horizontal arrows.

11 I believe that we call the category $\mathcal{C}^{\mathcal{D}}$ the functor category.

12 We actually just claimed this, and didn’t show it; but it took me all of 60 seconds to write it down including finding a working marker.
16 September 2011

Examples of Representability

Example: Let $F$ be the forgetful functor from $\mathcal{V}$ to $\mathcal{S}$. Note that $F$ is a covariant functor. We showed that $F$ is representable. That is, there is a vector space $U$ such that $F$ is naturally equivalent to $M_U = \text{Mor}_\mathcal{V}(U, -)$. Or restated again, we showed there is a vector space $U$ such that for all objects $W$ in $\mathcal{V}$, there is a natural bijection between $\tilde{W} = F(W)$ and $M_U(W) = \text{Mor}_\mathcal{V}(U, W)$. In fact, we can say that $\mathbb{R}$ represents $F$, i.e., that $F$ is naturally equivalent to $M_\mathbb{R}$. We define the natural transformation $\Phi : M_\mathbb{R} \to F$ via $\Phi_W : \text{Mor}_\mathcal{V}(\mathbb{R}, W) \to W$ is given by $L \mapsto L(1)$. It’ll be a homework problem to actually check that $\Phi_W$ is a bijection for all objects $W$ in $\mathcal{V}$ and also that $\Phi$ is natural.

Example: Now, let $W_1$ and $W_2$ be fixed objects in $\mathcal{V}$. We’ll define $F$ to be the contravariant functor from $\mathcal{V}$ to $\mathcal{S}$ which is given by $F(W) = \text{Mor}_\mathcal{V}(W_1, W) \times \text{Mor}_\mathcal{V}(W_2, W)$, and $F(f)$ will be given by $(\lambda_1, \lambda_2) \mapsto (\lambda_1 \circ f, \lambda_2 \circ f)$. This functor is also representable. That is, on objects, $F$ is equivalent to $\mathcal{S}$. But again, we didn’t actually show the natural transformation, and I don’t feel like typing the details of the setup.

Example: Let $\mathcal{F} = \{ W_i : i \in I \}$ be a family of objects in $\mathcal{V}$. We define a contravariant functor $F$ from $\mathcal{V}$ to $\mathcal{S}$ similarly to the previous example. That is, on objects, $F(W) = \prod_{i \in I} \text{Mor}_\mathcal{V}(W, W_i)$ and given a morphism $L : W \to W'$, we define $F(f)$ to be the map from $F(W')$ to $F(W)$ which is given by

$$\prod_{i \in I} \lambda'_i : i \mapsto \prod_{i \in I} \lambda'_i \circ L : i \in I.$$

However, this functor is not representable if $\sum_{i \in I} \dim W_i = \infty$, as the vector space we would want it to be representable by (namely $U = \prod_{i \in I} W_i$ is not an object in $\mathcal{V}$).

Comment: Grothendieck had a solution to this issue of non-representability. The solution basically boils down to embedding the category into a larger category where the object you want exists. We’ll start explaining this with the Yoneda Lemma next time.

19 September 2011

Yoneda Lemma

Yoneda Lemma Setup: Let $\mathcal{C}$ be a category. We can define a covariant functor $F$ from $\mathcal{C}$ to $\mathcal{C}^{\mathcal{S}}$ where $\mathcal{C}^{\mathcal{S}}$ is the category of contravariant functors $\mathcal{C}$ to $\mathcal{S}$. On objects, we define $F(C) = M^C$. Given a morphism $f \in \text{Mor}_\mathcal{C}(C, D)$ we define $F(f)$ to be the natural transformation $F(f) : M^C \to M^D$. In particular, if $B$ is an arbitrary object in $\mathcal{C}$, then we have $(F(f))(B) : M^C(B) \to M^D(B)$ or equivalently $(F(f))(B) : \text{Mor}_\mathcal{C}(B, C) \to \text{Mor}_\mathcal{C}(B, D)$ is given by $g \mapsto f \circ g$.

Yoneda Lemma: $F$ as defined above is a fully faithful functor.

Proof. We need to check four things here. They are:

1. $F(f)$ is a natural transformation:
   Let $A, B$ be objects in $\mathcal{C}$ with a morphism $g : B \to A$. We must show the following diagram commutes:

   $\begin{align*}
   M^C(A) \xrightarrow{M^C(g)} & M^C(B) \\
   F(f)(A) \xleftarrow{} & F(f)(B) \\
   M^D(A) \xrightarrow{M^D(g)} & M^D(B)
   \end{align*}$

---

13 This is because the dimensions are equal, so a basis must map to a basis to get injectivity.

14 See Fact on 12 September.

15 Recall that $M^C$ is a contravariant functor.
So let \( \varphi \in M^C(A) = \text{Mor}_C(A,C) \). Then we have \((F(f)(B) \circ M^C(g))(\varphi) = F(f)(B)(\varphi \circ g) = f \circ \varphi \circ g \). Similarly, we get \((M^D(g) \circ F(f)(A))(\varphi) = M^D(g)(f \circ \varphi) = f \circ \varphi \circ g \), so that the diagram commutes. However, this is “obvious” as \( M^C(g) \) and \( M^D(g) \) act by composing with \( g \) on the right, and \( F(f)(A) \) and \( F(f)(B) \) act by composing with \( f \) on the left, and composition is associative.

2. \textbf{F is a covariant functor}: Let \( C \) be an object in \( C \), and let \( 1_C \) be the identity morphism on \( C \) in \( C \). Then, \( F(1_C) \) is a natural transformation from \( M^C \) to \( M^C \). So let \( B \in \text{Ob}(C) \), then \( F(1_C)(B) : M^C(B) \rightarrow M^C(B) \) is given by \( g \mapsto g \circ 1_C = g \). Thus, \( F(1_C) = 1_{F(C)} \). We now need to look at compositions. So let \( f \in \text{Mor}_C(A,B) \) and \( g \in \text{Mor}_C(B,C) \). Then we want to show that \( F(g \circ f) = F(g) \circ F(f) \). For any object \( D \) in the category \( C \), then \( F(g \circ f)(D) : M^A(D) \rightarrow M^C(D) \) is given by composition with \( g \circ f \) on the left, so we get that \( h \mapsto (g \circ f) \circ h \). Similarly, \( F(f)(D) : M^B(D) \rightarrow M^C(D) \) is given by composition with \( f \) on the left, so \( h \mapsto f \circ h \), and \( F(g)(D) : M^A(D) \rightarrow M^B(D) \) is given by composition with \( g \) on the left, so \( h \mapsto g \circ h \). Now, if we have \( h \in M^A(D) \), then \( (F(g) \circ F(f))(h) = F(g)(f \circ h) = g \circ (f \circ h) \). However, composition is associative, and so we have that \( F(g \circ f) = F(g) \circ F(f) \).

3. \textbf{F is faithful}: Let \( C,D \) be objects in \( C \) and consider the map \( \text{Mor}_C(C,D) \rightarrow \text{Mor}_{C^S}(M^C,M^D) \) which is given by \( f \mapsto F(f) \). We must show that this map is injective. So let \( g,h \in \text{Mor}_C(C,D) \) such that \( g \neq h \). We must show that \( F(g) \neq F(h) \). We'll show this on \( C \). So consider \( F(g)(C), F(h)(C) : M^C(C) \rightarrow M^D(C) \). Then, \( F(g)(C)(1_C) = g \circ 1_C = g \neq h = h \circ 1_C = F(h)(C)(1_C) \), so that \( F(g)(C) \neq F(h)(C) \) and hence \( F(g) \neq F(h) \).

4. \textbf{F is full}: Again, Let \( C,D \) be objects in \( C \) and consider the map \( \text{Mor}_C(C,D) \rightarrow \text{Mor}_{C^S}(M^C,M^D) \) which is given by \( f \mapsto F(f) \). We must show that this map is surjective. So let \( \eta \in \text{Mor}_{C^S}(M^C,M^D) \). We'll set \( \alpha = \eta(C)(1_C) \). Note first that \( \eta(C) : M^C(C) \rightarrow M^D(C) \) so that \( \alpha \in \text{Mor}_C(C,D) \). We now claim that \( F(\alpha) = \eta \). To show this, let \( A \) be an object in \( C \) and \( \varphi \in \text{Mor}_C(A,C) \). Then as \( \eta \) is a natural transformation, we know the following diagram commutes:

\[
\begin{array}{ccc}
M^C(C) & \xrightarrow{\eta(C)} & M^D(C) \\
\varphi \downarrow & & \downarrow M^D(\varphi) = \varphi^* \\
M^C(A) & \xrightarrow{\eta(A)} & M^D(A)
\end{array}
\]

Now, tracing the identity morphism on \( C \) will give us what we want. Note here that the red equality is due to the definition of \( \alpha \), the blue equality is due to the diagram commuting, and the green equality is due to the definition of \( F(\alpha) \).

Thus the diagram tells us that \( \eta(A)(\varphi) = F(\alpha)(A)(\varphi) \) and so we have that \( \eta = F(\alpha) \) as desired so that the map is surjective.

\[ \square \]

\textbf{Representability and Free Groups}

\textbf{Example}: Let \( X \) be a set. We’ll define a covariant functor \( F_X \) from \( \text{Ab} \) to \( S \). On objects, \( F_X(A) = \text{Mor}_S(X,A) \) and on morphisms, if \( g : A \rightarrow B \), then \( F_X(g) : F_X(A) \rightarrow F_X(B) \) is given by \( \varphi \mapsto g \circ \varphi \). We wonder now if \( F_X \) is representable. It is, and I’ll show how we got there in class.

\textit{Proof}. We started by assuming that \( F_X \) is representable and seeing what that meant about the functor and about the object that represents it.

- So we’ll assume that \( B \) represents \( F_X \), i.e. that \( F_X \) is naturally equivalent to \( M_B \). Let \( \Phi : M_B \rightarrow F_X \) be the natural transformation.
- Then in particular we’d have \( \Phi_B : M_B(B) \rightarrow F_X(B) \) which is given by \( 1_B \mapsto \Phi_B(1_B) = \varphi \), where \( \varphi \) is simply defined to be the image of \( \Phi_B \) applied to the identity on \( B \).
- However, we really want to know what \( \Phi \) is in general. So let \( D \) be an abelian group, and \( g : B \rightarrow D \) a group homomorphism. We create the following commutative diagram to help us figure out what \( \Phi_B(D) \) is.
\[
\begin{array}{ccc}
M_B(B) & \xrightarrow{M_B(g)} & M_B(D) \\
\Phi_B & & \Phi_D \\
F_X(B) & \xrightarrow{F_X(g)} & F_X(D)
\end{array}
\]

- Tracing the element \(1_B\) tells us what we need, namely, that \(\Phi_D(g) = g \circ \varphi = g_*(\varphi)\). See the below diagram where the red equality is what will make the diagram commute.

\[
\begin{array}{ccc}
1_B & \xrightarrow{g_*(1_B)} & g \\
\varphi & & \downarrow \Phi_D \\
g_*(\varphi) & = g \circ \varphi & = \Phi_D(g)
\end{array}
\]

- Claim: The pair \((B, \varphi: X \to B)\) satisfies the following universal property: for any abelian group \(D\) and any set map \(\psi: X \to D\) there is a unique homomorphism \(h_\psi: B \to D\) such that the following diagram commutes:

\[
\begin{array}{ccc}
B & \xrightarrow{h_\psi} & D \\
\varphi & & \downarrow \psi \\
X & & 
\end{array}
\]

\textit{Sub-Proof.} This proof was fairly simple and was based entirely on the fact that we’re assuming that \(\Phi\) is a natural equivalence, i.e., that \(\Phi_D\) is an isomorphism of sets (which is just a bijection). \(\square\)

▷ COMMENT: The pair \((B, \varphi)\) exists, and is referred to as the free abelian group on the set \(X\).

▷ COMMENT: The above shows that the free abelian group on the set \(X\) represents the functor \(F_X\).

▷ CONSTRUCTION/DEFINITION: A much more explicit construction of a free abelian group can also be given. Here, we did this as the free abelian group on the set \(X\) is \(B = \bigoplus_{x \in X} \mathbb{Z}\), with the map \(\varphi: X \to B\). More generally, if \(\{B_x: x \in X\}\) is a family of abelian groups such that \(B_x = \mathbb{Z}\) for all \(x \in X\), then \(B = \bigoplus_{x \in X} B_x\) and \(\varphi: X \to B\) is given by \(x \mapsto e_x\) where \(e_x: X \to \mathbb{Z}\) is the map \(e_x(y) = \delta_{xy} = \begin{cases} 1, & x = y \\ 0, & x \neq y. \end{cases}\)

With all this, we denote the canonical inclusions by \(\tilde{\pi}_x: B_x \to B\).

▷ CLAIM: We claim now that \(B\) is a free abelian group, i.e. that it satisfies the appropriate universal property. The idea is to either:

- Show directly that \((B, \varphi)\) satisfies the universal property \(\textbf{OR}\)
- Use the universal property of \(B\) as a categorical coproduct (sum) to show that \((B, \varphi)\) satisfies the universal property of a free abelian group.

23 September 2011

FREE GROUPS & COPRODUCTS

▷ CLAIM: \((B, \varphi)\) as defined in the last class is a free abelian group, that is, it satisfies the following universal property: given any set map \(\Psi: X \to D\), where \(D\) is an abelian group, there is a unique homomorphism \(h_\Psi: B \to D\) such that the following diagram commutes:

\[
\begin{array}{ccc}
B & \xrightarrow{h_\Psi} & D \\
\varphi & & \downarrow \Psi \\
X & & 
\end{array}
\]

\textit{Proof.} We did most of the details of this in class. However, we used the fact that \(B\) is a categorical coproduct, and that basically gave us what we wanted, so I’m going to not rewrite down the details since neither existence nor uniqueness seemed at all tricky. \(\square\)
Definition: Let $X$ be a set, $F$ a group, and $\varphi : X \to F$ a set map. We say $(F, \varphi)$ is a free group on the set $X$ if for every group $G$ and every map $\Psi : X \to G$, there exists a unique homomorphism $h_\Psi : F \to G$ such that the diagram below commutes.

\[
\begin{array}{ccc}
F & \xrightarrow{h_\Psi} & G \\
\varphi \downarrow & & \downarrow \Psi \\
X & \xrightarrow{} & \end{array}
\]

Fact: Coproducts and free groups exist in the category of groups.

Proposition: Let $A$ and $B$ be groups with $A \cap B = \emptyset$ (for simplicity). Define the free product $A \circ B = A \star B$ to be the set of sequences $(a_1, \ldots, a_m)$ for $m \geq 0$ such that $a_i \in (A \setminus \{1_A\}) \cup (B \setminus \{1_B\})$ and such that if $a_i \in A$, then $a_{i+1} \notin A$ and if $a_i \in B$ then $a_{i+1} \notin B$. Then $A \circ B$ is a group under the following:

- $1_{A \circ B}$ is the unique sequence of length 0, namely $()$,
- $(a_1, \ldots, a_m)^{-1} = (a_m^{-1}, \ldots, a_1^{-1})$, and
- $\overline{a b} = (a_1, \ldots, a_m) \cdot (b_1, \ldots, b_n) = \begin{cases} (a_1, \ldots, a_m, b_1, \ldots, b_n) & \text{if } a_m, b_1 \text{ are in different groups, } A, B \\ (a_1, \ldots, a_m b_1, \ldots, b_n) & \text{if } a_m, b_1 \in A \text{ (or } B), \text{ and } a_m b_1 \neq 1_A \text{ or } 1_B \\ (a_1, \ldots, a_{m-1}) \cdot (b_2, \ldots, b_n) & \text{if } a_m b_1 = 1_A \text{ or } 1_B \end{cases}$

Proof. We discussed the ideas behind this proof in the next class, but I don’t think that any of them are really worth typing up. Basically, these things make sense. The only difficulty arose in showing associativity,\(^{16}\) and a sort of clever induction argument made it not so bad.

26 September 2011

Comments:
- $A \circ B = B \circ A$
- We have the obvious injective homomorphisms: \(^{17}\) $\pi_A : A \to A \circ B$, and $\pi_B : B \to A \circ B$ where $x \mapsto (x)$ for $x \in A$ (or $x \in B$ as is appropriate), and obviously in each case the identity maps to the identity in $A \circ B$ which is the sequence of length 0.
- Given any group homomorphisms, $\varphi_* : * \to G$ for $* = A, B$, then we claim there is a unique\(^{18}\) group homomorphism $\varphi : A \circ B \to G$ such that the following diagrams commute for $* = A, B$:

\[
\begin{array}{ccc}
A \circ B & \xrightarrow{\varphi} & G \\
\downarrow \pi_* & & \downarrow \varphi_* \\
* & \xrightarrow{} & * 
\end{array}
\]

In fact, we define $\varphi$ as follows: Clearly we set $\varphi((())) = 1_G$. Also, $\varphi((x)) = \varphi_*(x)$ where $x \in *$ and $* = A, B$, and in general, if $x = (x_1, \ldots, x_n)$, then $\varphi(x) = \varphi((x_1)) \cdots \varphi((x_n))$. There are a bunch of cases to check it is a homomorphism, but it seems clear enough without checking them. Also, the fact that the diagrams commute seems clear, so I won’t write down any of the details of either.\(^{19}\)

Corollary: Let $A$ and $B$ be groups, which we regard as having disjoint sets of elements. Then $(A \circ B, \pi_A, \pi_B)$ is a coproduct of $A$ and $B$ in the category of groups.

Proof. It only remains to show uniqueness of the map $\varphi$. However, this is easy to show since the diagrams must commute and $\varphi$ must be a homomorphism, so I’ll omit the details from these typed notes.

Examples: The coproduct of $A = \mathbb{Z}/2\mathbb{Z} = \{0, 1_A\}$ and $B = \mathbb{Z}/2\mathbb{Z} = \{1_B, -1\}$ contains the elements: $A \circ B = \{(), (1_A), (-1), (1_A, -1), (-1, 1_A), (1_A, -1, 1_A), (-1, 1_A, -1, 1_A), \ldots\}$. Note here that there are exactly two elements of each length. However, in the category of abelian groups, the coproduct is the direct sum, namely $A \oplus B = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ which is the Klein Vier Group.\(^{20}\)

Lemma: Let $X_1$, and $X_2$ be disjoint sets, and assume $(F_i, \varphi_i)$ is a free group on $X_i$ for $i = 1, 2$. Then $F_1 \circ F_2$ is the free group on the set $X = X_1 \cup X_2$ with respect to the map $\varphi : X \to F_1 \circ F_2$ defined by $x \mapsto \pi_i(\varphi_i(x))$.

---

\(^{16}\)as always!

\(^{17}\)that they are injective and homomorphisms is “clear.”

\(^{18}\)I haven’t asserted uniqueness, but it will be unique. It’s the freeness that makes it unique.” –B.H.

\(^{19}\)I’m aware that this silly $*$ notation sucks, but I’m lazy and don’t want to do everything twice for both $A$ and $B$.

\(^{20}\)Vier is 4 in German.
28 September 2011

**Free (Abelian) Groups**

**Lemma:** If $X_1, X_2$ are disjoint sets, and $(F_i, \varphi_i)$ is a free group on $X_i$ for $i = 1, 2$, then $F_1 \circ F_2$ is a free group on $X = X_1 \cup X_2$.

*Proof.* Let $\overline{\varphi}_i : F_i \to F_1 \circ F_2$ be the coproduct canonical homomorphisms, and define $\varphi : X \to F_1 \circ F_2$ via $x \mapsto \overline{\varphi}_i(\varphi_i(x))$ for $x \in X_i$. We need to show that $(F_1 \circ F_2, \varphi)$ is a free group on $X$. So let $\psi : X \to G$ be any set map to any group $G$. We must show there is a unique homomorphism $h_\psi : F_1 \circ F_2 \to G$ such that $h_\psi \circ \varphi = \psi$. In order to work the coproduct into the proof, we'll need homomorphisms $\Gamma_i : F_i \to G$. Let $\Gamma_i$ be the unique homomorphism guaranteed by the universal property of $F_i$ free from the set map $\gamma_i : X_i \to G$, where $\gamma_i = \psi|_{X_i}$. The maps $\Gamma_i$ then induce the map $\Gamma : F_1 \circ F_2 \to G$ since $F_1 \circ F_2$ is a coproduct. Set $h_\psi = \Gamma$. We must show that $h_\psi \circ \varphi = \psi$ and that this map is unique. So, let $x \in X = X_1 \cup X_2$. Without loss of generality (WLOG), let $x \in X_1$. Then,

$$(h_\psi \circ \varphi)(x) = \Gamma \circ \overline{\varphi}_i \circ \varphi_i(x) = \Gamma_1 \circ \varphi_1(x) = \gamma_1(x) = \psi|_{X_1}(x) = \psi(x).$$

**Examples:**

1. The free group on the empty set is the trivial group.
2. The free group on $X = \{1\}$ is isomorphic to $\mathbb{Z}$.
3. Inductively, using the lemma, we have the the free group on a set $X = \{1, \ldots, n\}$ is $\mathbb{Z} \circ \ldots \circ \mathbb{Z}$.
4. It is possible to define a free group on an infinite set as well, and Lang describes this. It is similar in idea to what we’ve done so far, but is a bit messier.

**Lemma 1:** Let $(F, \varphi : X \to F)$ be a free group. Then $\varphi$ is injective, and $\varphi(X)$ generates $F$.

*Proof.* Notice that the injectivity is trivial if $|X| < 2$, so we may let $x_1, x_2$ be distinct elements of $X$. Define $\psi : X \to \mathbb{Z}/2\mathbb{Z}$ as $\psi(x) = \begin{cases} 1, & x \neq x_1 \\ 0, & x = x_1 \end{cases}$. Then by the universal property, there is a unique homomorphism $h_\psi : F \to \mathbb{Z}/2\mathbb{Z}$ such that $h_\psi \circ \varphi = \psi$. However, $\psi(x_1) \neq \psi(x_2)$, so we must have that $\varphi(x_1) \neq \varphi(x_2)$ due to the fact that $h_\psi \circ \varphi = \psi$. Next, let $G$ be the subgroup of $F$ generated by $\varphi(X)$. We'll show $G = F$. Consider the diagram below:

\[ \begin{array}{ccc} F & \xrightarrow{h_\varphi} & G \\ \varphi \downarrow & & \downarrow \varphi \\ X & \xleftarrow{i} & F \end{array} \]

Notice that by definition of $F$ as a free group, there is a unique homomorphism $h_\varphi : F \to F$ such that $h_\varphi \circ \varphi = \varphi$. As $1_F$ works for $h_\varphi$, then we must have that $1_F = i \circ h_\varphi$. Since $1_F$ is a bijection, then we must have that $i$ is surjective, meaning that $F \subseteq G$, and hence $F = G$.

**Lemma 2:** Let $(A, \varphi : X \to A)$ be a free abelian group. Then $\varphi$ is injective and $\varphi(X)$ generates $A$.

*Proof.* The proof is the same as the proof of Lemma 1, mutatis mutandis.

30 September 2011

**Free (Abelian) Groups**

**Example:** If $X$ is a set, then $A = \bigoplus_{x \in X} \mathbb{Z}$ together with $e : X \to A$ given by $x \mapsto e_x$ is a free abelian group, where $e_x : X \to \mathbb{Z}$ is given by $e_x(y) = 0$ for $y \neq x$, and $e_x(x) = 1$.

**Lemma 3:** Let $(A, \varphi : X \to A)$ be a free abelian group on $X$. Then every element $a \in A$ has a unique expression

$$a = \sum_{x \in X} m_x \varphi(x),$$

where $m_x \in \mathbb{Z}$.

---

21This is “obvious” once you draw the pictures, but there are too many to be worth putting in here.

22This is “obvious” once you draw the pictures, but there are too many to be worth putting in here.

23See Hungerford page xv. This is latin for (roughly) “by changing the things which (obviously) must be changed (in order that the argument will carry over and make sense in the present situation).”
Proof. Notice that existence here is due to Lemma 2 since \( \varphi(X) \) generates \( A \) as an abelian group. So we really only need to show uniqueness. Since \( \bigoplus_{x \in X} \mathbb{Z} e_x \) is a free abelian group, then we have homomorphisms \( h_e \) and \( h_\varphi \) such that \( h_e \circ \varphi = e \) and \( h_\varphi \circ e = \varphi \). Now, suppose \( \sum_{x \in X} m_x \varphi(x) = \sum_{x \in X} n_x \varphi(x) \). We'll apply \( h_e \) to get the following:

\[
\sum m_x e_x = \sum m_x h_e(\varphi(x)) = h_e \left( \sum m_x \varphi(x) \right) = h_e \left( \sum n_x \varphi(x) \right) = \sum n_x h_e(\varphi(x)) = \sum n_x e_x.
\]

We can apply these functions to any element \( y \in X \) to get that

\[
m_y = \sum m_x e_x(y) = \sum n_x e_x(y) = n_y
\]

for all \( y \in X \). Hence, the two expansions are equivalent, which gives us uniqueness. \qed

\( \triangleright \) Definition: A subset, \( B \), of an abelian group, \( A \), is a basis for \( A \) if \( B \) generates \( A \) in a unique way.

\( \triangleright \) Definition: If \( B \) is a basis for \( A \), then we say \( |B| \) is the rank of \( A \).

\( \triangleright \) Lemma 4: If \( (F, \psi : X \to F) \) is a free abelian group and we have a commutative diagram:

\[
\begin{array}{ccc}
F & \xrightarrow{\sim} & G \\
\downarrow{\psi} & & \downarrow{\varphi} \\
X & & \\
\end{array}
\]

then \( (G, \varphi) \) is free abelian on \( X \) as well.

\( \triangleright \) Proposition: If \( B \) is a basis for an abelian group \( A \), then \( (A, \varphi) \) is a free abelian group where \( \varphi : B \to A \) is the inclusion of \( B \) into \( A \).

Proof. Let \( (F, \psi) \) be a free abelian group on the set \( B \). Then we have the induced commutative diagram:

\[
\begin{array}{ccc}
F & \xrightarrow{h_\varphi} & A \\
\downarrow{\psi} & & \downarrow{\varphi} \\
B & & \\
\end{array}
\]

We now claim that in fact \( h_\varphi \) is an isomorphism. We'll first do surjectivity. As \( B = \varphi(B) \) generates \( A \), and \( \varphi(B) = \psi(h_\varphi(B)) \), then \( h_\varphi(F) \) contains \( B \), so that \( h_\varphi(F) = A \) since \( B \) is a basis for \( A \). Next, we'll do injectivity. Let \( f \in \ker(h_\varphi) \). Since \( \psi(B) \) generates \( F \), then we get \( f = \sum_{b \in B} m_b \psi(b) \) for some \( m_b \in \mathbb{Z} \). Now,

\[
0 = h_\varphi(f) = h_\varphi \left( \sum_{b \in B} m_b \psi(b) \right) \equiv \sum_{b \in B} m_b h_\varphi(\psi(b)) = \sum m_b \varphi(b),
\]

which means that \( m_b = 0 \) for all \( b \in B \), and hence \( f = 0 \), so that \( h_\varphi \) is injective. Applying Lemma 4 now completes the proof. \( \square \)

\( \triangleright \) Lemma 5: If we have a free abelian group \( (A, \varphi : X \to A) \) and a set \( Y \) with a bijection \( \beta : X \to Y \), then \( (A, \varphi \circ \beta^{-1}) \) is a free abelian group on \( Y \).

\( \triangleright \) Corollary: Let \( A \) be an abelian group. Let \( X \) be a set with a map \( \varphi : X \to A \). then \( (A, \varphi) \) is a free abelian group if and only if \( \varphi(X) \) is a basis for \( A \) and \( \varphi \) is injective.

\( \triangleright \) Fact: If \( X \) is an infinite set, and \( \text{Fin}(X) \) is the set of finite subsets of \( X \), then \( |X| = |\text{Fin}(X)| \).

3 October 2011

Free Groups, Group Actions

\( \triangleright \) Theorem: Let \( (A_i, \varphi_i : X_i \to A_i) \) be free abelian groups for \( i = 1, 2 \). Then \( A_1 \cong A_2 \) if and only if \( |X_1| = |X_2| \).

\(^{24}\)The proof here is “easy” if you draw the pictures.

\(^{25}\)The proof here is an application of the lemmas and the proposition.
Proof. \((\Leftarrow)\) Let \(\psi : X_1 \to X_2\) be a bijection. Since \((A_2, \varphi_2)\) is free abelian on \(X_2\), then \((A_2, \varphi_2 \circ \psi)\) is free abelian on \(X_1\) by Lemma 5. Thus, \(A_1 \cong A_2\) by the universal property of their both being free on \(X_1\).

\((\Rightarrow)\) Now, assume \(A_1 \cong A_2\), and let \(h : A_1 \to A_2\) be an isomorphism. Set \(2A_1 = \{2a|a \in A_1\}\) and note that \(2A_1 \triangleleft A_1\). Set \(\overline{A}_i = A_i/2A_i\). We claim now that \(h\) induces an isomorphism \(\overline{h} : \overline{A}_1 \to \overline{A}_2\). So set \(h(a) = \overline{h}(a)\). We first show this is well defined. Suppose \(a \in A_1\). Then \(a + b \in 2A_1\). Note that \(h(2A_1) = 2h(A_1) \subseteq 2A_2\) so that \(h(a) - h(b) \in 2A_2\) which gives \(\overline{h}(a) = \overline{h}(b)\). Next, we must show that \(\overline{h}\) is an isomorphism. In fact, we have the following commutative diagram:

\[
\begin{array}{ccc}
A_1 & \xrightarrow{h} & A_2 \\
\downarrow & & \downarrow \\
\overline{A}_1 & \xrightarrow{\overline{h}} & \overline{A}_2
\end{array}
\]

Since \(h\) and \(-\) are surjective, then so is \(-\circ h\). We claim then that ker\((-\circ h) = 2A_1\) and apply the first isomorphism theorem.\(^{26}\) Note that \((-\circ h)(2a) = 2\overline{h}(a) = \overline{0}\) in \(\overline{A}_2\) so that \(2A_1 \subseteq \ker(-\circ h)\). Now, suppose \((-\circ h)(a) = \overline{0}\). Then we have \(\overline{h}(a) = \overline{0}\) so that \(h(a) \in 2A_2\). So let \(h(a) = 2b\) for some \(b \in A_2\). But \(h\) is an isomorphism, so there exists some \(\beta \in A_1\) such that \(h(\beta) = b\). Thus, \(h(a) = 2h(\beta) = h(2\beta)\) so that \(a = 2\beta \in 2A_1\) since \(h\) is an isomorphism. Thus, \(\overline{h}\) is an isomorphism.

Now, for \(i = 1, 2\) we have the following:

\[
\overline{A}_i \cong \bigoplus_{x \in X_i} \mathbb{Z} = \bigoplus_{x \in X_i} \mathbb{Z} \cong \bigoplus_{x \in X_i} \mathbb{Z}/2\mathbb{Z},
\]

which gives the isomorphism \(\bigoplus_{x \in X_1} \mathbb{Z}/2\mathbb{Z} \cong \bigoplus_{x \in X_2} \mathbb{Z}/2\mathbb{Z}\). Now, if \(|X_1| < \infty\), then we get

\[
2^{|X_1|} = \bigoplus_{x \in X_1} \mathbb{Z}/2\mathbb{Z} = \bigoplus_{x \in X_2} \mathbb{Z}/2\mathbb{Z} = 2^{|X_2|}
\]

which means that \(|X_1| = |X_2|\). If, on the other hand, \(X_1\) (and hence also \(X_2\)) is infinite, then we have

\[
|X_1| = |\text{Fin}(X_1)| = \bigoplus_{x \in X_1} \mathbb{Z}/2\mathbb{Z} = \bigoplus_{x \in X_2} \mathbb{Z}/2\mathbb{Z} = |\text{Fin}(X_2)| = |X_2|
\]

which completes the proof. \(\Box\)

\(\triangleright\) **Comment:** We’re now going to move on from free groups and start discussing group actions. We’ll also briefly cover the Sylow Theorems, and will probably cover semi-direct products.

\(\triangleright\) **Definition:** Let \(G\) be a group and \(X\) a set. An action of \(G\) on \(X\) is a map \(\alpha : G \times X \to X\) (usually we write \(g \cdot x\) or simply \(gx\) for the action of \(g\) on the set element \(x\)) such that

1. \(1_G \cdot x = x\) for all \(x \in X\), and
2. \(g_1 \cdot (g_2 \cdot x) = (g_1g_2) \cdot x\) for all \(x \in X\) and for all \(g_1, g_2 \in G\).

\(\triangleright\) **Definition:** We say the orbit of an element \(x \in X\) is the set \(G \cdot x = \{g \cdot x|g \in G\}\).

\(\triangleright\) **Definition:** Let \(x \in X\). Then the stabilizer of \(x\) is \(\text{Stab}_G(x) = \{g \in G|g \cdot x = x\}\). Notice here that the stabilizer is a subgroup of \(G\).

\(\triangleright\) **Comment:** Sometimes the notation \(G_x\) is used for the stabilizer of \(x\), but that notation sucks given our notation for the orbits!

\(\triangleright\) **Definition:** We say an action is transitive if it has a single orbit. Equivalently, if for some \(x \in X\) (but really it will be true for all \(x \in X\)), we have \(G \cdot x = X\).

\(^{26}\) Apparently the isomorphism theorems are due to Emmy Noether?
Math 901 Notes

5 October 2011

More Group Actions; Starting Semi-Direct Products

Recall: We have two equivalent definitions of an action being transitive. The first is that there is a unique orbit. The second is that given any two elements \( x, y \in X \), there is a group element \( g \in G \) such that \( g \cdot x = y \).

Example: We discussed the action of \( S^1 \) on \( \mathbb{C} \) where \( S^1 \) acts on \( \mathbb{C} \) via regular multiplication in \( \mathbb{C} \). Here, this action is not transitive, but each orbit is a circle centered about the origin.

Theorem: (In particular a version of Cayley’s Theorem) Let \( \varphi : G \times X \to X \) be an action of a group \( G \) on a set \( X \), let \( x \in X \), and \( H = \text{Stab}_G(x) \).

1. Then \( \varphi \) induces a homomorphism \( \Phi : G \to \text{Perms}(X) \) which is given by \( g \mapsto \pi_g \) where \( \pi_g(y) = g \cdot y \).
2. If the action is transitive, then \( \ker \Phi \subseteq H \) and moreover, \( \ker \Phi = \bigcap_{g \in G} gHg^{-1} \) and lastly, \( \ker \Phi \) contains every subgroup \( N \leq G \) such that \( N \triangleleft G \) and \( N \subseteq H \).

Proof. We’ll show each part:

1. We first need to show that \( \pi_g \) is actually a permutation for every \( g \in G \). So note that given \( g \in G \), then \( (\pi_g \circ \pi_{g^{-1}})(x) = \pi_g(g^{-1} \cdot x) = g(g^{-1}x) = e_Gx = x \) and \( (\pi_g \circ \pi_{g^{-1}})(x) = g^{-1}(gx) = e_Gx = x \) so that \( \pi_g \) is a bijection for each \( g \) and hence an element of \( \text{Perms}(X) \).

Next, we need to show that \( \Phi \) is a homomorphism. That is, we need to show that \( \pi_{g_1g_2} = \Phi(g_1g_2) = \Phi(g_1) \circ \Phi(g_2) = \pi_{g_1} \circ \pi_{g_2} \). So let \( x \in X \). We’ll show that both permutations send \( x \) to the same place. Now, \( \pi_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = \pi_{g_1}(\pi_{g_2}(x)) = \pi_{g_1} \circ \pi_{g_2}(x) \). Thus, \( \Phi \) is a homomorphism.

2. First, we’ll show that \( \ker \Phi \subseteq H \). So let \( a \in \ker \Phi \). Then \( \pi_a = 1_X \) so that \( \pi_a(y) = a \cdot y = y \) for any \( y \in X \). Hence, \( a \cdot x = x \) so that \( a \in \text{Stab}_G(x) = H \).

Next, we need to show that \( \ker \Phi \subseteq \bigcap_{g \in G} gHg^{-1} \). So let \( a \in \ker \Phi \) and let \( g \in G \). It is clearly enough to show that \( a \in gHg^{-1} \).

If \( a \in \ker(\Phi) \) then \( a(gx) = gx \) so that \( g^{-1}agx = x \). This means that \( g^{-1}ag \in H \) and so \( a \in gHg^{-1} \).

Next, we’ll show the other inclusion \( \ker \Phi \supseteq \bigcap_{g \in G} gHg^{-1} \). So let \( b \in \bigcap_{g \in G} gHg^{-1} \), and let \( y \in X \). Then \( y = \gamma x \) for some \( \gamma \in G \) since the action is transitive. Also, \( b = \gamma h \gamma^{-1} \) for some \( h \in H \) by choice of \( b \). Thus, multiplying both sides of these two equations together gives \( by = \gamma h \gamma^{-1} \gamma x \). Simplifying the right hand side gives \( by = \gamma h x = \gamma x = y \). Thus, \( \Phi(b) = \pi_b = 1_X \) so that \( b \in \ker(\Phi) \).

Lastly, we must show that \( \ker(\Phi) \) is the largest normal subgroup of \( G \) which is contained in \( H \). So let \( N \triangleleft G \) with \( N \subseteq H \), and choose any \( g \in G \). Then \( N = gNg^{-1} \subseteq gHg^{-1} \). Thus, \( N \subseteq \bigcap_{g \in G} gHg^{-1} \subseteq \ker(\Phi) \) which completes the proof.

Corollary: If a group \( G \) acts transitively on a finite set \( X \) and if \( |G| > n! \) where \( n = |X| > 1 \), then \( G \) has a nontrivial normal subgroup, \( N \).

Proof. We didn’t prove this in class, but I’ll do it now. Since \( |G| > |X|! = |\text{Perms}(X)| \), then the homomorphism \( \Phi \) from part 1 of the theorem cannot be injective. This means that \( \ker(\Phi) \geq \{1_G\} \). By part 2 of the theorem above, we know that \( H = \text{Stab}_G(x) \) contains \( \ker(\Phi) \) for any \( x \in X \). Now, since the action is transitive, and \( X \) has more than one element, then there must be at least one \( g \in G \) such that \( gx \neq x \). Hence, \( H \leq G \), so that \( \ker(\Phi) \) is a proper subgroup of \( G \) as we now have \( \{1_G\} \leq \ker(\Phi) \leq H \leq G \). Since the kernel of any group homomorphism is a normal subgroup, then we have that \( \ker(\Phi) \) is a non-trivial normal subgroup.

Semi-Direct Products: We can do this in a more general setting, but we’ll give an example first to illustrate the idea.

Example: Let \( G \) be a group, with subgroups \( N, H \) such that \( N \cap H = \{1_G\} \) and \( N \triangleleft G \). Then, \( NH = \{nh : n \in N, h \in H\} \) is a subgroup of \( G \). We let \( H \) act on \( N \) by conjugation, and can refer to \( NH \) as an internal semi-direct product.
More Group Actions

More Group Actions

10 October 2011

Proposition: Let $G$ be a finite group acting on a finite set $X$. Let $n$ be the number of orbits. Let $f : G \to \mathbb{Z}$ be a map where $f(g)$ is the number of fixed points of $g$, i.e., $f(g) = |\{x \in X : gx = x\}|$. Then $n|G| = \sum_{g \in G} f(g)$.

Proof. Let $X_1, \ldots, X_n$ be the distinct orbits, and set $f_i(g) = |\{x \in X_i : gx = x\}|$. Note then that $f(g) = \sum_{i=1}^n f_i(g)$.

Let $\Gamma_i$ be a “correspondence” in $G \times X_i$. In particular, let $\Gamma_i = \{(g, x) \in G \times X_i | gx = x\}$. We then have the following diagram where $\pi_1$ and $\pi_2$ are the usual projection maps:

$$
\begin{array}{ccc}
\Gamma_i \subseteq G \times X_i & \xrightarrow{\pi_1} & G \\
\downarrow \pi_2 & & \\
X_i & & 
\end{array}
$$

Consider $\pi_2|_{\Gamma_i} : \Gamma_i \to X_i$. Note that this map is surjective as $(e_G, x) \in \Gamma_i$ for all $x \in X_i$. Also, the fibers are

$$
(p_2|_{\Gamma_i})^{-1}\{(x)\} = \{(g, x) : gx = x\} = \text{Stab}_G(x) \times \{x\},
$$

and

$$
(p_1|_{\Gamma_i})^{-1}\{(g)\} = \{(g, x) : x \in X_i \text{ and } gx = x\}.
$$

27 We didn’t actually show this operation turned $N \times H$ into a group, but it isn’t hard to show, and some people even did it as homework. The only tricky part is determining that $(n, h)^{-1} = (\Phi(h^{-1})(n^{-1}), h^{-1})$.

28 This seems not too hard to show and part of it may have been done by some people for homework.

29 This was actually stated the previous day, but proved this day, so it’s listed here.
More Group Actions & the Class Equation

We now assume that $G$ acts on $X_i$ and so $|\{g \in G : x \in X_i\}| = f_i(g)$. The fibers of a map are always disjoint, and their union is the domain; hence, $\sum_{g \in G} f_i(g) = |\Gamma_i| = \sum_{x \in X_i} |\text{Stab}_G(x)|$. Recall that $|G| = |\text{Stab}_G(x)| \cdot |G : x|$. Hence, $\sum_{g \in G} f_i(g) = |\Gamma_i| = \sum_{x \in X_i} |G|/|X_i| = |G|$. Now, we add these up over $i$ to get

$$\sum_{g \in G} f(g) = \sum_{g \in G} \sum_{i=1}^n f_i(g) = \sum_{i=1}^n \sum_{g \in G} f_i(g) = \sum_{i=1}^n |G| = n|G|.$$

\[\square\]

\begin{itemize}
  \item \textbf{Corollary:} Say $G$ is a finite group acting transitively on a finite set $X$ with $|X| > 1$. Then there exists an element $g \in G$ which is fixed-point free, that is, so that $gx \neq x$ for all $x \in X$. In the language of the previous proposition, this says there is an element $g \in G$ such that $f(g) = 0$.
  
  \textbf{Proof.} Suppose not, then for each $g \in G$ there exists an $x_g \in X$ such that $g \cdot x_g = x_g$. Or equivalently, $f(g) \geq 1$ for every $g \in G$. Since the action is transitive, $|G| = \sum_{g \in G} f(g)$. This means that $f(g) = 1$ for every $g \in G$, but this is a contradiction since $f(1_G) = |X| \geq 2$.
  
  \[\square\]
  
  \item \textbf{Corollary:} Let $G$ be a group, $H$ a subgroup such that $H \leq G$. If $G$ is a finite group, then $\bigcup_{g \in G} gHg^{-1} \subseteq G$.
  
  \textbf{Proof.} We know $G$ acts on the left cosets of $H$ by left multiplication. Set $X = \{gH\}_{g \in G}$. Since $H \leq G$, then we have that $|X| > 1$. Also, note that this action is transitive, and choose any $a \in G$. Then $a \in gHg^{-1}$ for some $g \in G$ if and only if $g^{-1}ag \in H$, which happens if and only if $ag \in gH$, or equivalently if and only if $a$ is in the stabilizer of $gH$ under the group action, i.e. $a \cdot gH = gH$. Now, let $S = \bigcup_{g \in G} gHg^{-1}$. Then $a \in S$ if and only if $f(a) \geq 1$, where as before, $f(a)$ is the number of fixed points of $a$ under the action, or equivalently, $f(a)$ is the number of conjugates $gHg^{-1}$ which contain $a$. However, by the previous corollary, there is some $b \in G$ such that $f(b) = 0$. Hence, $b \notin S$. \[\square\]
\end{itemize}

\section*{12 October 2011}

\begin{itemize}
  \item \textbf{More Group Actions & the Class Equation}
  
  We now provide an alternate proof for the Corollary proved last time:
  
  \textbf{Proof. Alternate Proof:} Let $G$ act on the set of conjugates of $H$ by conjugation, and set $X = \{gHg^{-1}\}$.\footnote{This IS an action.} Note that $\text{Stab}_G(H) = \{g \in G : gHg^{-1} = H\} = N_G(H)$.$^1$ Recall that $|gHg^{-1}| = |H|$ for all $g \in G$, and that $1_H \in gHg^{-1}$ for all $g \in G$. Let $n$ be the number of conjugates of $H$, i.e. $n = |X| = |G|/|\text{Stab}_G(H)| = |G|/|N_G(H)|$.
  
  If $n = 1$, then $H < G$ and for all $g \in G$, we have $gHg^{-1} = H$, so clearly $\bigcup_{g \in G} gHg^{-1} \subseteq G$. So suppose $n \neq 1$. We have the following computation:

  $$\left|\bigcup_{g \in G} gHg^{-1}\right| \leq n(|H| - 1) + 1 = \frac{|G|}{|N_G(H)|} (|H| - 1) + 1 = \frac{|G|}{|N_G(H)|} |H| - \frac{|G|}{|N_G(H)|} + 1.$$

  Now, $N_G(H) \leq G$, $|H|/|N_G(H)| \leq 1$, and $|G|/|N_G(H)| = n \geq 2$, and so from the computation we get that

  $$\left|\bigcup_{g \in G} gHg^{-1}\right| \leq |G| - 2 + 1 = |G| - 1 < |G|.$$

  \[\square\]
  
  \item \textbf{Class Equation:} Let $G$ act on itself via conjugation $\cdot h = ghg^{-1}$. This gives us a homomorphism $\Phi : G \to \text{Aut}(G)$ with kernel the center of the group, which we recall is denoted $Z(G)$. The image of $\Phi$ is a subgroup of $\text{Aut}(G)$ which is known as the group of inner automorphisms, and is sometimes denoted $\text{Inn}(G)$. For $h \in G$, we have that $\text{Stab}_G(h) = \{g \in G : g = h\}$ is the centralizer of $h$ in $G$. More generally, the centralizer of a subset $S \subseteq G$ is $\text{C}_G(S) = \{g \in G : gs = sg \text{ for all } s \in S\}$. Note here that $\text{C}_G(G) = Z(G)$.
  
  We now assume that $G$ is a finite group, and that $X_1, \ldots, X_n$ are the disjoint orbits of the group under the conjugation action. For each $i$, choose any $x_i \in X_i$. Then we have the class equation:

  $$|G| = \sum_{i=1}^n |X_i| = \sum_{i=1}^n |G : \text{C}_G(x_i)|.$$

  \footnote{Recall that $N_G(H)$ is the normalizer of $H$ in $G$.}
\end{itemize}
However, this is more commonly written as follows and separates out the singleton orbits:

$$|G| = |Z(G)| + \sum |G : C_G(x_i)|$$

where now the sum is taken over those $i$’s such that $C_G(x_i) \leq G$.

\begin{itemize}
\item **PROPOSITION:** Let $G$ be a finite group, and $H$ a subgroup of index 2. Then $H \triangleleft G$.
\item **Proof.** Let $g \in G$. If $g \in H$, then obviously $gH = Hg$. However, if $g \notin H$, then $gH$ and $Hg$ are both disjoint from $H$, and since the index is 2, we must have that $gH = Hg$. Hence, $gH = Hg$ for all $g \in G$, and so $H$ is normal in $G$.
\end{itemize}

\textbf{14 October 2011}

**Group Actions & Sylow Theorems & Nilpotent Groups**

\begin{itemize}
\item **Corollary:** If $G$ is a finite group and has an element with exactly two conjugates, then $G$ has a non-trivial, proper, normal subgroup.
\item **Proof.** Let $g \in G$ be an element with exactly two conjugates, then under conjugation of the group on itself, $\text{Stab}_G(g)$ has index 2. So by the proposition, $\text{Stab}_G(g)$ is a proper normal subgroup of $G$. It remains to show that $\text{Stab}_G(g)$ is a non-trivial, proper subgroup. However, this is easy since $g \in \text{Stab}_G(g)$ and $g \neq 1_G$ since $1_G$ has only itself as a conjugate, and so $\text{Stab}_G(g)$ is a non-trivial, proper, normal subgroup.
\end{itemize}

\begin{itemize}
\item **PROPOSITION:** Let $G$ be a finite group, and let $p$ be the smallest prime such that $p$ divides the order of the group. If $G$ has a subgroup, $H$, of index $p$, then $H \triangleleft G$.
\item **Proof.** We didn’t prove this in class, but I’ll do it here anyways. Let $X$ be the set of left cosets of $H$ in $G$. Then, $G$ acts on $H$ by left multiplication, and this action is clearly transitive. Then the homomorphism, $\Phi$, given by Cayley’s theorem has kernel $\ker(\Phi) \subseteq H$ as we have that $H = \text{Stab}_G(H)$ since $gH = Hg$ if and only if $g \in H$. Our goal is to get that $\ker(\Phi) = H$. Now, we know that $\text{Perms}(X)$ is a group of size $p!$, and so we must have that $|G/\ker(\Phi)|$ divides $p!$. However, if $r$ divides the index of $\ker(\Phi)$ in $G$, then $r$ divides the order of $G$ since the index divides the order of the group. Since $p$ is the smallest prime that divides the order of the group, and no number larger than $p$ divides $G/\ker(\Phi)$, then we must have that $|G/\ker(\Phi)|$ is either 1 or $p$. We now do the following computation:

$$|G/\ker(\Phi)| = |G : \ker(\Phi)| = |G : H|/|H : \ker(\Phi)| = p[H : \ker(\Phi)] \geq p.$$ 

Thus, we must have that $|G : \ker(\Phi)| = p$, so that $\ker(\Phi) = H$ since we already knew that $\ker(\Phi) \subseteq H$. Hence $H$ is normal in $G$.
\end{itemize}

\begin{itemize}
\item **Definition:** Let $p$ be a prime. A finite group, $G$, is called a $p$-group if $|G| = p^n$ for some $n \in \mathbb{N}$.
\item **“Trivial” Example:** The trivial group is a $p$-group for all primes $p$.
\item **Lemma:** Let $G$ be a non-trivial $p$-group for some prime $p$. Then $|Z(G)| > 1$.
\item **Proof.** We apply the class equation. The size of the group $G$ is the size of its center plus the sum of the order of the orbits of elements having conjugates other than themselves. Note that $p$ divides the order of the group, and $p$ divides the order of each orbit of elements having conjugates other than themselves. Thus, $p$ must divide the order of the center of $G$, and so $|Z(G)|$ is at least $p$, and hence greater than 1.
\end{itemize}

\begin{itemize}
\item **Cauchy’s Theorem:** Let $G$ be a finite group, and $p$ a prime such that $p$ divides the order of $G$. Then $G$ has an element of order $p$.
\item **Proof.** From class notes: “A beautiful proof can be given using $\mathbb{Z}/p\mathbb{Z}$ acting via cyclic permutations on a subset of $G \times \cdots \times G$, $p$ times.” –B.H.
\end{itemize}

\begin{itemize}
\item **Definition:** Let $p$ be a prime. A subgroup of order $p^n$ of a finite group, $G$, is called a $p$-subgroup.
\item **Definition:** Let $G$ be a finite group of order $p^5 \cdot m$ where $p$ is prime and $(m, p) = 1$. Then a $p$-subgroup of $G$ that has order $p^n$ is called a Sylow $p$-subgroup.
\item **Sylow’s Theorem(s):** Let $G$ be a finite group of order $p^n \cdot m$ where $p$ is prime and $p \nmid m$.
\begin{enumerate}
\item $G$ has a Sylow $p$-subgroup.
\end{enumerate}

\[32\]This proof is different from the one given in class, but makes more sense to me.

\[33\]Oh My!

\[34\]Groups with no non-trivial, proper, normal subgroup are called simple, so we could just say that then $G$ is not a simple group.

\[35\]The subgroup $H$ and the stabilizer $H$ from the theorem are now the same thing.

\[36\]Hahaha!

\[37\]This seems to indicate that we don’t need to know the proof, but at some point, I think I should understand and type up a real proof.
2. If $Q$ is a $p$-subgroup of $G$ and $P$ is a Sylow $p$-subgroup, then $Q \subseteq gPg^{-1}$ for some $g \in G$. In particular, any two Sylow $p$-subgroups of a group are conjugate.

3. If $n_p$ denotes the number of Sylow $p$-subgroups, then $n_p \equiv 1 \pmod{p}$ and $n_p | m$.

**Definition:** A sequence of subgroups $G_1 \leq G_2 \leq \ldots \leq G_s = G$ of a group $G$ is called an abelian tower if $G_i \triangleleft G_{i+1}$ and $G_{i+1}/G_i$ is abelian and both statements hold for all $i$.

**Comment:** Nilpotent and Solvable groups be defined based upon special abelian towers.

---

**19 October 2011**

**Useful Fact:** Let $P$ be a Sylow $p$-subgroup of a finite group $G$. Then $N_G(N'_G(P)) = N_G(P)$.

**Proof.** We have that $P \triangleleft N_G(P) \triangleleft N_G(N'_G(P))$ but remember that normality is not a transitive relation. So, we know that $P$ is the unique Sylow $p$-subgroup of $N_G(P)$ by part 2 of the Sylow Theorem(s). We easily get the inclusion $N_G(P) \subseteq N_G(N'_G(P))$, so we need to show the other. Let $g \in N_G(N'_G(P))$. Then $gP^{-1} \triangleleft gN'_G(P)g^{-1} = N_G(P)$ by choice of $g$. Thus, $P = gPg^{-1}$ since $P$ is the unique Sylow $p$-subgroup of $N_G(P)$. In particular, this means that $g \in N_G(P)$ and so we get the other inclusion.

**Lemma:** Let $G$ be a finite group. Assume the Sylow subgroup of $G$ are all normal. Then $G$ is the direct product of its Sylow subgroups.

**Proof.** Let $|G| = p_1^{r_1} \cdots p_s^{r_s}$ where $p_i$ are distinct primes and assume $r_i > 0$ for all $i$. By part 1 of Sylow’s Theorem(s), there exists a Sylow $p_i$-subgroup, $P_i$, for each $i$. Then we need to show that $G \cong P_1 \times \cdots \times P_s$. If $s = 1$, then the statement is trivial since $G = P_1$ is a $p_1$-group, so assume $s > 1$. Define $\theta : P_1 \times \cdots \times P_s \rightarrow G$ by $((g_1, \ldots, g_s)) \mapsto g_1 \cdots g_s$. We need to check three things:

- $\theta$ is a HOMOMORPHISM: Let $(g_1, \ldots, g_s)$ and $(h_1, \ldots, h_s)$ be elements of $P_1 \times \cdots \times P_s$. Then, $\theta((g_1, \ldots, g_s) \cdot (h_1, \ldots, h_s)) = \theta((g_1h_1, \ldots, g_1h_s)) = g_1h_1 \cdots g_sh_s$.

Also, $\theta((g_1, \ldots, g_s)) \cdot \theta((h_1, \ldots, h_s)) = (g_1 \cdots g_s) \cdot (h_1 \cdots h_s)$. We get that this is a homomorphism once we show that $gh = hg$ whenever $g \in P$, $h \in P_j$, and $i \neq j$. Note that $ghg^{-1}h^{-1} = (ghg^{-1})h^{-1} \in P_j$ since $h \in P_j \triangleleft G$.

- Inclusion: $\theta$ is injective.

- Surjectivity: $\theta$ is surjective.

**Definition(s):** Let $G$ be a group. Consider the following sequence of quotients:

$$G = G_0 \twoheadrightarrow G_1 \twoheadrightarrow G_2 \twoheadrightarrow \ldots$$

where $G_{i+1} = G_i/Z(G_i)$. We get a sequence then of surjective homomorphisms $\sigma_j : G \rightarrow G_j$. Let $C_0(G) := (e_G)$, and $C_j(G) := \ker(\sigma_j)$.

Then $C_0(G) < C_1(G) < C_2(G) < \ldots$ is called the ascending central series. We’ll show next time that it is an abelian tower. The group $G$ is nilpotent if $G = C_i(G)$ for some $i \in \mathbb{N}$. Equivalently, we can say that $G$ is nilpotent if $|G_i| = 1$ for some $i \in \mathbb{N}$.

**Example:** Any abelian group is nilpotent. This is obvious since $G/Z(G) = G_1$ is the trivial group.

---

38This second bit is usually (in my oh-so-humble experience) stated that $n_p$ divides the order of the group, but given the first part, the two are equivalent.

39We did a terrible job doing it this day, but next time it actually makes sense!
21 October 2011

\textbf{Nilpotent Groups}

\begin{itemize}
\item Note: The following are fairly easy facts to show about the set of group homomorphisms $f : A \to B$ and $g : B \to C$.
\item 1. $f(A) \cong A/\ker(f)$
\item 2. $\ker(f) \subseteq \ker(g \circ f)$
\item 3. $f(\ker(g \circ f)) \cong \ker(g \circ f)/\ker(f)$
\item 4. $\ker(g \circ f) = f^{-1}(\ker(g))$
\item 5. If $f$ is surjective, then $f(\ker(g \circ f)) = f(f^{-1}(\ker(g))) = \ker(g)$ by applying fact 4 from this list. Applying this to the 3rd fact gives us
\begin{equation}
\ker(g) \cong \ker(g \circ f)/\ker(f)
\end{equation}
\end{itemize}

\begin{itemize}
\item PROPOSITION: The ascending central series defined in the last class is an abelian tower.
\end{itemize}

\begin{proof}
Let $f : G \to G_i$, and $g : G_i \to G_{i+1}$ be the given surjections. Then $\ker(f) = C_i(G)$, $\ker(g) = Z(G_i)$, and $\ker(g \circ f) = C_{i+1}(G)$ all by definition or simple observation. Plugging these into equation (1) gives us $Z(G_i) \cong C_{i+1}(G)/C_i(G)$. In particular, this means that the ascending central series is an abelian tower. \qed
\end{proof}

\begin{itemize}
\item FACTS:
\begin{itemize}
\item If $p$ is prime, then any finite $p$-group, $G$, is nilpotent.
\item A product of nilpotent groups is nilpotent.
\item A group $G = B(1) \times \ldots \times B(r)$ where each $B(i)$ is a finite $p_i$-group for primes $p_i$ is nilpotent.
\end{itemize}
\end{itemize}

\begin{proof}
Let $G$ be a nilpotent group, and let $H \leq G$. Then $H \leq N_G(H)$.
\end{proof}

\begin{proof}
Let $n$ be the largest index such that $C_n(G) \subseteq H$. We know such an $n$ exists since $G$ is nilpotent. Then choose any $b \in C_{n+1}(G) \setminus H$. Since $C_{n+1}(G)/C_n(G) \cong Z(G_n) \cong Z(G/C_n(G))$, then $bC_n(G) \in Z(G/C_n(G))$. Let $h \in H$. Then $bhC_n(G) = (bC_n(G))(hC_n(G)) = (hC_n(G))(bC_n(G)) = hbC_n(G)$ and this all takes place in the group $G/C_n(G)$. Thus, there is some $a \in C_n(G) \subseteq H$ so that $bha = hb$. Thus, as $h$ and $a$ are both elements of $H$, we get, $b^{-1}hb = ha \in H$. Thus, we get $b \in H$. But we also had $b \notin H$, and so $H \subseteq N_G(H)$ as desired. \qed
\end{proof}

\begin{itemize}
\item THEOREM: A finite group $G$ is nilpotent if and only if it is the product of its Sylow subgroups.
\end{itemize}

\begin{proof}
(\Rightarrow) If $G$ is a product of its Sylow $p$-subgroups for primes $p$ which divide the order of the group, then $G$ is a finite product of nilpotent groups, and hence is nilpotent.

(\Leftarrow) Say $G$ is a finite nilpotent group. It is enough to show that each Sylow subgroup is normal in $G$, because if so, then $G$ is a product of its Sylow subgroups (see the first Lemma from 19 Oct). If $G$ is a $p$-group, then we’re clearly done. So, we assume otherwise, and let $P \leq G$ be a Sylow $p$-subgroup of $G$. From the USEFUL FACT at the beginning of the 19th of October, we know that $N_G(N_G(P)) = N_G(P)$. Also, by the Lemma just previous to this, we know that if $N_G(P) \leq G$, then we’d have $N_G(P) \leq N_G(N_G(P))$ which would be a contradiction, and so we must have that $N_G(P) = G$. Thus, $P \triangleleft G$ and that completes the proof. \qed
\end{proof}

24 October 2011

\textbf{Solvable Groups}

\begin{itemize}
\item DEFINITION: A group $G$ is \textbf{solvable} if it has an abelian tower of the following form:
$$
\langle e_G \rangle = G_m \lhd G_{m-1} \lhd \ldots \lhd G_0 = G,
$$
where $G_i/G_{i+1}$ is abelian for all $i$. A series of this form is called a \textbf{solvable series} for $G$.
\end{itemize}

\begin{itemize}
\item NOTE: It is clear that nilpotent groups are all solvable. We’ll see later that not all solvable groups are nilpotent.
\end{itemize}

\footnote{I’ve modified this proof a bit from the one given in class so that I understand it better.}
Feit-Thompson Theorem: (Conjectured by Burnside) Every finite group of odd order is solvable.\footnote{Thompson got a fields medal for this!}

Derived Series: Let $G^{(1)}$ (also written $G'$) be the commutator subgroup of $G$, $[G, G]$, and call it the first derived subgroup of $G$. Recursively, $G^{(i+1)}$ is called the $i + 1$st derived subgroup, and is the first derived subgroup of the $i$th derived subgroup, that is, $G^{(i+1)} = (G^{(i)})'$. Note that $G \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \ldots$, and that $G^{(i)}/G^{(i+1)}$ is abelian (we know this from the homework). This sequence of subgroups is an abelian tower known as the derived series.

Note: If there is an $m$ such that $G^{(m)} = (e_G)$, then $G$ is solvable.

Proposition: Let $G$ be a group. Then $G$ is solvable if and only if the derived series terminates at the identity.\footnote{The proof of this is embedded in the proof of the Useful Fact.}

Proof. ($\Leftarrow$) This is clear! ($\Rightarrow$) Assume $G$ is solvable. Then there is an abelian tower $G_m = (e_G) < G_{m-1} < \ldots < G_0 = G$. Since, $G_0/G_1$ is abelian, then $G_1 \supseteq G^{(1)}$. We can inductively show that $G^{(i)} \subseteq G_i$. Then we get $G^{(m)} \subseteq G_m = (e_G)$, which completes the proof since $G_i / G_{i+1}$ being abelian means that $G_i' \subseteq G_{i+1}$ for all $i$. Thus, $G^{(i+1)} = (G^{(i)})' \subseteq G_i' \subseteq G_{i+1}$.\qed

Useful Fact: Let $G$ be a group, and $N < G$, then $G$ is solvable if and only if $N$ and $G/N$ are.\footnote{This is not always part of the definition, but it will be for our class.}

Proof. ($\Rightarrow$) Assume $G$ is solvable, then $N^{(i)} \subseteq G^{(i)}$, so if $G^{(m)} = (1_G)$, then so does $N^{(m)}$, and so $G$ being solvable implies that $N$ is solvable. Next, if $f : G \to H'$ is any group homomorphism, then $f(G^{'i}) \subseteq H'$, and if $f$ is surjective, then $f(G') = H'$. Thus, under the quotient homomorphism $q : G \to G/N$, we get $q(G^{(i)}) = (G/N)^{(i)}$, so that $G$ being solvable implies that $G/N$ is also solvable.

($\Leftarrow$) We'll build an abelian tower for $G$ out of towers for $N$ and $G/N$. First, let $N_m = (e_G) < N_{m-1} < \ldots < N_0 = N$ be a solvable series for $N$, and let $G_m = (e_G) < G_{m-1} < \ldots < G_0 = G/N$ be a solvable series for $G/N$. Then $G_i = q^{-1}(G_i)$. Then $G_i / G_{i+1} \cong (G_i / G_{i+1})/G_0 = G_i / G_0$ is abelian. Note that $G_0 = G$, and $G_s = N$. Then we have the following as a solvable series for $G$, which completes the proof:

$$(e_G) = N_m < \ldots < N_0 = N = G_s < \ldots < G_0 = G.$$\qed

Corollary: If $G$ is solvable, then any subgroup of $G$ and every homomorphic image of $G$ is solvable.

Example: Not every solvable group is nilpotent. The group $S_3$ is solvable. This is because $A_3 < S_3$, and $A_3$ is abelian, and every abelian group is solvable. Also, $S_3 / A_3 \cong \mathbb{Z}/2\mathbb{Z}$ which is abelian and hence also solvable. Thus by the Useful Fact we've got that $S_3$ is solvable. However, $S_3$ is not nilpotent! Note here that $Z(S_3) = (1_S)$, and so the ascending central series is constant. Alternately, the sylow subgroups of $S_3$ are of order 3 and 8, but $S_3$ has order 6, and so it cannot be the direct product of its Sylow subgroups.

26 October 2011

Finish Solvable Groups & Start Rings (Fields)

Corollary: $S_n$ is not solvable for $n \geq 5$.

Corollary: $A_n$ is not solvable for $n \geq 5$.

Definition: A ring is an abelian group $(R, +)$ with a binary operation $\ast$ called multiplication such that

- $\ast$ is associative
- $R$ contains a multiplicative identity, denoted $1_R$ or 1.$^{43}$
- Multiplication distributes over addition on both the left and the right. That is, for $a, b, c \in R$, we have $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

Note: If we also have the $\ast$ is commutative, then we say that $R$ is a commutative ring.

Example: If $0 = 1$, then $R = \{0\}$.

Facts: Let $R$ be a ring, and $b \in R$. Then the following are easy to show from the properties.

- For any $b \in R$, we get $-b = (-1)b = b(-1)$.
- For any $b \in R$, we get $b0 = 0b = 0$.

Definition: We say a ring $R$ is a division ring if $1 \neq 0$ and for any $b \in R \setminus \{0\}$, there exists $b^{-1} \in R$ such that $bb^{-1} = b^{-1}b = 1$.

Definition: A commutative division ring is a field.

Example: The real quaternions are a division ring. As a set they are $Q = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$, where 1 is a multiplicative identity for $Q$, addition works like a vector space, and $ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j$, and $i^2 = j^2 = k^2 = -1$. We also have that multiplication is associative and distributes over addition. It is possible in this ring to find inverses of any non-zero element in a manner similar to the field $\mathbb{C}$, but in this ring, multiplication is not commutative, so it is not a field.

$^{41}$Thompson got a fields medal for this!

$^{43}$This is not always part of the definition, but it will be for our class.
We started today by proving the comment from the previous day.
▷ FACT: If $\alpha$ is algebraic over a field $F$, then

$$[F(\alpha) : F] = [F[\alpha] : F] = \dim_F(F[\alpha]) = \dim_F\left(\frac{F[x]}{(\text{Irr}(\alpha, F, x))}\right) = \deg(\text{Irr}(\alpha, F, x)) < \infty.$$ 

However, if $\alpha$ is transcendental, then $[F(\alpha) : F] = \infty$.

▷ QUESTION: Why is the set of elements in a field $E$ which are algebraic over a subfield $F$ actually a subfield of $E$?\(^{44}\)

▷ THEOREM: Let $k$ be a field, $L$ an algebraically closed field such that there is an embedding $\sigma : k \to L$. Let $E$ be an algebraic extension field of $k$. Then there is a homomorphism $\sigma' : E \to L$ such that the diagram below commutes.\(^{45}\)

$$\begin{array}{ccc}
E & \xrightarrow{\sigma} & L \\
\downarrow{\sigma'} & & \downarrow{\sigma} \\
E & & L
\end{array}$$

▷ COROLLARY: Any two algebraic closures, $A, B$, of a field $k$ are isomorphic over $k$; that is, there exists an isomorphism $\phi : A \to B$ such that $\phi|_k = id_k$.\(^{46}\)

▷ NOTATION: Lang denotes the algebraic closure of a field $k$ by $k^a$. Note that $k^a$ can technically be any algebraically closed field containing $k$ which is algebraic over $k$. The point of the corollary is that the algebraic closure of a field is unique up to isomorphism.

---

2 November 2011

▷ RECALL: A field $K$ is **algebraically closed** if every non-constant polynomial $f \in K[x]$ has a root in $K$. We say an algebraically closed field $K$ which contains $k$ is an **algebraic closure** of $k$ if $K$ is algebraic over $k$.\(^{47}\)

▷ COMMENTS:
- The only algebraic extension of an algebraically closed field, $k$, is the field $k$ itself.
- Every field has an algebraic closure.

▷ DEFINITION: We say a field extension $k \subseteq K$ is an **algebraic closure** if $K$ is algebraically closed, and the extension is algebraic.

▷ EXAMPLE: $\mathbb{C}$ is algebraically closed, but is not the algebraic closure of $\mathbb{Q}$. Instead, $\mathbb{Q}^a = \{z \in \mathbb{C} : z$ is algebraic over $\mathbb{Q}\}$.

▷ DEFINITION: Let $S \subseteq k[x]$ be a set of non-constant polynomials. Then $K$ is a **splitting field** for $S$ if every element of $S$ splits (factors into linear factors in $K[x]$) and if $K$ is generated over $k$ by the roots of elements of $S$.

▷ EXAMPLES:
1. $\mathbb{C}$ is a splitting field for $x^2 + 1$ over $\mathbb{R}$.
2. $\mathbb{Q}(\sqrt{2})$ is a splitting field over $\mathbb{Q}$ for $x^2 - 2$.
3. $\mathbb{Q}(\sqrt{2})$ is not a splitting field over $\mathbb{Q}$ for $x^3 - 2$ since it’s missing the complex roots.
4. For any field $k$, $k^a$ is the splitting field over $k$ for the set $S = \{\text{all positive degree polynomials in } k[x]\}$.

▷ DEFINITION: A field extension $k \subseteq K$ is **normal** if $K$ is a splitting field of some set of polynomials of positive degree in $k[x]$.

▷ THEOREM: If $A$ and $B$ are extension fields of $k$, and $A, B$ are splitting fields for the same set $S$ of polynomials, then $A \cong B$ over $k$. That is, there is an isomorphism $\phi : A \to B$ such that $\phi|_k = id_k$.

▷ THEOREM: Consider fields $k \subseteq K \subseteq k^a$. The following three statements are equivalent:
1. $K$ is a normal extension of $k$.
2. Every homomorphism $h : K \to k^a$ such that $h|_k = 1_k$ is an automorphism of $K$.
3. Every irreducible polynomial in $k[x]$ which has a root in $K$ actually splits (factors linearly) in $K$.

---

4 November 2011

▷ EXAMPLE: The extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ is a finite algebraic extension, but it is not a normal extension since not all of the roots of $\text{Irr}(\sqrt[3]{2}, \mathbb{Q}, x)$ are in $\mathbb{Q}(\sqrt[3]{2})$. We also explained that $\mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}^2, \sqrt[3]{2}^3] \cong \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}^2, \sqrt[3]{2}^3]$. Hence, there are at least three homomorphisms over $\mathbb{Q}$ from $\mathbb{Q}(\sqrt[3]{2})$ to $\mathbb{Q}^a$.\(^{44}\)

\(^{44}\)We justified this, but I won’t here.

\(^{45}\)Cited as review.

\(^{46}\)We partially proved the corollary given the theorem, but it is one of those non-interesting proofs where you just follow your nose.

\(^{47}\)The algebraic closure of a field $k$ is frequently denoted $\overline{k}$.

\(^{48}\)This was cited from Lang, and is review.

\(^{49}\)Also cited and review.
PROPOSITION: Let $k$ be a field, and let $\alpha \in k^a$. Let $f(x) = \text{Irr}(\alpha, k, x)$. Then the number of distinct homomorphisms from $k[\alpha]$ to $k^a$ over $k$ is equal to the number of distinct roots of $f(x)$ in $k^a$.

Proof. This is just a sketch! It is easy to show that if $h$ is such a homomorphism, then $f(h(\alpha)) = 0$ so that $h(\alpha)$ is also a root of $f(x)$. Since $h$ is determined by its value on $\alpha$, then it is clear that the number of homomorphisms over $k$ is no larger than the number of distinct roots of $f$ in $k^a$. Also, you can define a homomorphism by sending $\alpha$ to any of the other roots, so there are exactly as many homomorphisms over $k$ as there are distinct roots of the irreducible polynomial. \hfill $\blacksquare$

COROLLARY: The number of $k$–homomorphisms of $k[\alpha] \to k^a$ is no larger than $\deg \text{Irr}(\alpha, k, x)$ if $\alpha \in k^a$.

EXAMPLE: Let $k$ be a field, and $y$ and indeterminate, then $x^2 - y \in (k(y))[x]$ is irreducible. If $k$ has characteristic 2, then $x^2 - y = x^2 + y = (x + \sqrt{y})^2 \in (k(y))[x]$ and so $x^2 - y$ only has a single root in $k(y)^a$.

DEFINITION: Let $k$ be a field. We define a linear operator (known as the derivative) by $\frac{d}{dx} : k[x] \to k[x]$ via $\frac{d}{dx}ax^n = anx^{n-1}$ and by extending linearly.

COMMENTS:
- The derivative satisfies the Liebnitz rule: $\frac{d}{dx}(fg) = \frac{df}{dx}g + f \frac{dg}{dx}$
- If $k \subseteq E$ is an algebraic field extension, then $\frac{d}{dx}$ on $k[x]$ is the restriction of $\frac{d}{dx}$ on $E[x]$.
- We can use derivatives to detect polynomials with multiple roots since the linear factors aren’t unique and due to the Liebnitz rule! In particular, $\alpha$ is a multiple root of $f(x) \in k[x]$ if and only if the power of $(x - \alpha)$ in the factorization of $f(x)$ is strictly greater than one.
- If $k$ is a field of characteristic $p > 0$, then $\frac{d}{dx}x^p = px^{p-1} = 0$.

DEFINITION: Let $k \subseteq E$ be a field extension, and let $\alpha \in E$ be algebraic over $k$. We say $\alpha$ is separable over $k$ if $\text{Irr}(\alpha, k, x)$ does not have any multiple roots in $k^a$. An extension $k \subseteq E$ is separable if $E$ is algebraic over $k$ and every element of $E$ is separable over $k$.

DEFINITION: A finite algebraic extension is Galois if it is both normal and separable.

7 November 2011

FROBENIUS: Let $k$ be a field of characteristic $p > 0$. We get a homomorphism $F : k \to k$ given by $a \mapsto a^p$, which is called the Frobenius map. This is because in a field of characteristic $p$, we have $(a + b)^p = a^p + b^p$ and in any commutative ring $(ab)^p = a^pb^p$.

EXAMPLE: Let $k$ be a field, $f \in k[x]$ where $d = \deg f \geq 1$. If $f'(x) = 0$ (since $d > 1$, this means $k$ is a field of positive characteristic, say $p$), then $f$ is actually a polynomial in $x^p$ and $p|d$. If we work over $k^a$, then we can take $p^{th}$ roots of elements of $k$, and so $f'(x) = 0$ gives that $f(x) = (h(x))^p$ where $h \in k^a[x]$.

COROLLARY: Let $k$ be a field. Let $\alpha$ be algebraic over $k$, and let $f = \text{Irr}(\alpha, k, x)$. The following are equivalent:
- $\alpha$ is not separable over $k$,
- $f'(\alpha) = 0$, and
- $f'(x) = 0$.

COROLLARY: Let $k \subseteq K$ be an algebraic field extension, and assume that the characteristic of $k$ is zero, (and hence so is the characteristic of $K$). Then $K$ is a separable extension of $k$.

PROPOSITION: Let $k \subseteq K$ be finite fields. Then the extension is separable and normal.

Proof. Let $p > 0$ be the characteristic of both fields. Then the prime field is $\mathbb{Z}/p\mathbb{Z}$. This means $K$ is a $\mathbb{Z}/p\mathbb{Z}$ vector space of dimension $\dim_{\mathbb{Z}/p\mathbb{Z}} K = m$. That is, $K \cong \bigoplus_{i=0}^{m-1} \mathbb{Z}/p\mathbb{Z}$. This gives that $|K| = p^m$, and $[K : \mathbb{Z}/p\mathbb{Z}] = m$. Let $K^* = K \setminus \{0\}$ be the multiplicative group of $K$. Then $|K^*| = p^m - 1$ and by Lagrange’s Theorem, $\alpha |K^*| = 1_K$ for all $\alpha \in K^*$. Thus, $x^{p^m - 1} - 1$ is a polynomial of degree $p^m - 1$ with $p^m - 1$ distinct roots. Hence, $x^{p^m - 1}$ and $x^{p^m} - x$ are separable and the roots of the second polynomial are the $p^m$ distinct elements of $K$. Now, for any $\alpha \in K$, we get that $\text{Irr}(\alpha, k, x)$ divides $x^{p^m} - x$, and so $\text{Irr}(\alpha, k, x)$ cannot have any multiple roots, so that $\alpha$ is separable over $k$ so that the extension is normal (since $\alpha$ was arbitrary). Moreover, the extension is normal since $x^{p^m} - x$ splits in $K[x]$ and the set of roots of $x^{p^m} - x$ is precisely $K$, and so it generates $K$ over $k$. \hfill $\blacksquare$

50The proof is not really difficult and I’ve seen it before, so I’m omitting it here.
51This is almost entirely a direct application of the previous corollary.
9 November 2011

\[ \text{SEPARABLE DEGREE} \]

\[ \text{Definition: } \text{Let } K \text{ be a finite algebraic extension of a field } k \text{ so that } k \subseteq K \subseteq k^a. \text{ We define the separable degree of } K \text{ over } k, \text{ denoted } [K : k], \text{ to be the cardinality of the set of } k-\text{homomorphisms } K \to k^a. \]

\[ \text{Note/Example: } \text{For simple algebraic extensions, the separable degree } [k(\alpha) : k], \text{ is the number of distinct roots of } \text{Irr}(a, k, x). \text{ If } \alpha \text{ is separable, then the separable degree and the degree } [k(\alpha) : k] \text{ are equal. If } \alpha \text{ is not separable, then we know } \text{char}(k) = p > 0 \text{, and if } f(x) = \text{Irr}(\alpha, k, x), \text{ then } f'(x) = 0, \text{ so that } f(x) = (h(x))^p \text{ for some } h(x) \in k^a[x]. \text{ In fact, there is an } m > 0 \text{ such that } f(x) = (g(x))^p_m \text{ where } g \text{ has no multiple roots. In this case, } [k(\alpha) : k] = \deg g(x) \text{ and } [k(\alpha) : k] = \deg f(x) = (\deg g(x)) \cdot p^m = p^m[k(\alpha) : k]. \text{ We refer to } \frac{[k(\alpha) : k]}{[k(\alpha) : k]}, \text{ as the inseparable degree and denote it } [k(\alpha) : k]. \]

\[ \text{Theorem: } \text{Let } k \subseteq E \subseteq K \subseteq k^a \text{ be fields and assume } K \text{ is a finite extension of } k. \text{ Then the separable degree is multiplicative and finite. Moreover, } [K : k], \text{ divides } [K : k]. \text{ Here, we call } [K : k]/[K : k] \text{ the inseparable degree and denote it by } [K : k]. \]

\[ \text{Proof. Let } S_{K/k}, \text{ be the set of } k-\text{homomorphisms } K \to k^a. \text{ So } |S_{K/k}| = [K : k]. \text{ Similarly, } S_{K/E}, \text{ is the set of } E-\text{homomorphisms } K \to k^a \text{ and } S_{E/k}, \text{ is the set of } k-\text{homomorphisms } E \to k^a. \text{ Thus, } |S_{K/E}| = [K : E] \text{ and } |S_{E/k}| = [E : k]. \text{ For each } k-\text{homomorphism } \gamma : E \to k^a \text{ pick an extension } \tilde{\gamma} : k^a \to k^a \text{ so that } \tilde{\gamma}|_E = \gamma. \text{ We’ll now define a map} \]

\[ \varphi : S_{K/k} \to S_{K/E} \times S_{E/k} \]

\[ \text{via} \]

\[ h \mapsto \left( \left( \frac{h|_E}{h} \right)^{-1} \circ h, h|_E \right). \]

\[ \text{Showing that this map is bijective will complete the proof. We’ll do this by finding an inverse to } \varphi. \text{ Let} \]

\[ \lambda : S_{K/E} \times S_{E/k} \to S_{K/k} \]

\[ \text{be given by } (h, g) \mapsto \tilde{g} \circ h. \text{ Note that } h : K \to k^a \text{ is a } E-\text{homomorphism} \text{ (and hence a } k-\text{homomorphism)} \text{ and } \tilde{g} : k^a \to k^a \text{ is a } k-\text{homomorphism and so their composition exists as written and is a } k-\text{homomorphism from } K \text{ to } k^a, \text{ and hence an element of } S_{K/k} \text{ as desired. We now must show that compositing these two maps is the identity in both directions. We have} \]

\[ (\lambda \circ \varphi)(h) = \lambda(\varphi(h)) = \lambda \left( \left( \frac{h|_E}{h} \right)^{-1} \circ h, h|_E \right) = \tilde{h}|_E \circ \left( \left( \frac{h|_E}{h} \right)^{-1} \circ h \right) = h \]

\[ \text{and similarly since } h|_E = \text{id}_E \text{ and } \tilde{g}|_E = g, \text{ we get} \]

\[ (\varphi \circ \lambda)((h, g)) = \varphi(\lambda((h, g))) = \varphi(\tilde{g} \circ h) = \left( \left( \left( \frac{\tilde{g} \circ h}{\tilde{g} \circ h} \right)^{-1} \circ \left( \tilde{g} \circ h \right), h \right) \right) = \left( \left( \frac{\tilde{g}|_E}{\tilde{g}|_E} \right)^{-1} \circ \tilde{g} \circ h, h \right) = (h, g). \]

\[ \text{Thus, we have that } |S_{K/k}| = |S_{K/E}| \cdot |S_{E/k}| \text{ as desired to give that separable degree is multiplicative.} \]

\[ \text{Now, since } K \text{ is a finite extension of } k, \text{ we can pick a finite set of elements } \alpha_1, \ldots, \alpha_r \text{ so that } \]

\[ k \subseteq k(\alpha_1) \subseteq k(\alpha_1, \alpha_2) \subseteq \ldots \subseteq k(\alpha_1, \ldots, \alpha_r) = K. \]

\[ \text{Using what we learned about simple extensions in the Note/Example, we have that} \]

\[ |S_{K/k}| = |S_{K/k(\alpha_1, \ldots, \alpha_{r-1})}| \cdot |S_{k(\alpha_1, \ldots, \alpha_{r-1})/k(\alpha_1, \ldots, \alpha_{r-2})}| \cdot \ldots \cdot |S_{k(\alpha_1)/k}| \]

\[ = [K : k(\alpha_1, \ldots, \alpha_{r-1})] \cdot [k(\alpha_1, \ldots, \alpha_{r-1}) : k(\alpha_1, \ldots, \alpha_{r-2})] \cdot \ldots \cdot [k(\alpha_1) : k]. \]

\[ ^{52}\text{We’ll justify this first thing on the 14th of November using the idea of separable degree.} \]
As each of the factors\(^{53}\) if finite, then so is their product, \(|S_{K/k}|\). That is, \([K : k]_s < \infty\). The fact that separable degree in general divides the regular degree is a combination of the facts that degree is multiplicative, separable degree is multiplicative, and that for a simple extension separable degree divides the regular degree. \(\square\)

11 November 2011

\(\square\) **Definition:** Let \(k \subseteq E\) be a field extension. We define \(\text{Aut}_k(E) := \{f \in \text{Aut}(E) : f|_k = \text{id}_k\}\).

\(\square\) **Note:** Every field homomorphism is injective\(^{54,55}\). Also note that for any field extension \(k \subseteq E\), the set \(\text{Aut}_k(E)\) is actually a group under composition.

\(\square\) **Comment:** Given any field \(k\), the group \(\text{Aut}_k(k^a)\) acts on the roots of any polynomial \(f \in k[x]\). By letting \(\sigma \in \text{Aut}_k(k^a)\), we get the following commutative diagram where the two vertical(ish) maps are the obvious inclusion map(s):

\[
\begin{array}{ccc}
  k^a & \xrightarrow{\sigma} & k^a \\
  \downarrow & & \downarrow \\
  k & & k \\
  \end{array}
\]

This map \(\sigma\) can then be extended to an automorphism of \(k^a[x]\) so that the similar diagram commutes where again the vertical(ish) maps are the obvious inclusion map(s):

\[
\begin{array}{ccc}
  k^a[x] & \xrightarrow{\overline{\sigma}} & k^a[x] \\
  \downarrow & & \downarrow \\
  k[x] & & k[x] \\
  \end{array}
\]

By definition if \(f = \sum_{i=1}^{n} a_i x^i \in k^a[x]\), then \(\overline{\sigma}(f) = \sum_{i=1}^{n} \sigma(a_i) x^i\). Because \(\overline{\sigma}\) is a homomorphism, we have \(\overline{\sigma}(f + g) = \overline{\sigma}(f) + \overline{\sigma}(g)\) and \(\overline{\sigma}(fg) = \overline{\sigma}(f) \overline{\sigma}(g)\). So if \(f \in k[x]\) is monic, then in \(k^a[x]\) we have that \(f(x) = (x - \alpha_1) \ldots (x - \alpha_m)\) and so \(f = \overline{\sigma}(f(x)) = (x - \sigma(\alpha_1)) \ldots (x - \sigma(\alpha_m))\) which means that \(\sigma\) permutes the roots of \(f\), and this gives the action.

\(\square\) **Note:** The action need not be transitive; however, if \(f \in k[x]\) is irreducible, then the action will be transitive. We show that now: If \(\alpha_1, \alpha_2\) are roots in \(k^a\) of an irreducible polynomial \(f\), then \(k[\alpha_1] \cong k[x]/(f) \cong k[\alpha_2]\) where the maps are given by \(x \mapsto \alpha_i\) and called \(\tau\) and \(\sigma\) respectively. So there is a \(k\)–isomorphism \(\sigma \tau^{-1} : k[\alpha_1] \rightarrow k[\alpha_2]\) given by \(\alpha_1 \mapsto \alpha_2\), and this can be extended to all of \(k^a\) to get a \(k\)–homomorphism \(\gamma : k^a \rightarrow k^a\) such that \(\gamma|_{k[\alpha_1]} = \sigma \tau^{-1}\).

Thus, \(\gamma(\alpha_1) = \alpha_2\) and the action is transitive as desired.

\(\square\) **Corollary:** If \(f \in k[x]\) is a (monic),\(^{56}\) irreducible polynomial that factors over \(k^a\) as \(f(x) = (x - \alpha_1)^{m_1} \ldots (x - \alpha_r)^{m_r}\). Then \(m_1 = \ldots = m_r\).

**Proof.** Choose any \(\alpha_i, \alpha_j\) roots of the polynomial \(f\). For simplicity, make them \(\alpha_1\) and \(\alpha_2\) in the expansion of \(f\) in \(k^a[x]\). Then, there is some \(k\)–homomorphism \(\gamma : k^a \rightarrow k^a\) such that \(\gamma(\alpha_1) = \alpha_2\) by the transitivity of the action as explained above. Then \(\gamma(f) = f\) as \(f \in k[x]\) and \(\gamma\) is a \(k\)–homomorphism. However, we also see that

\[
(x - \alpha_1)^{m_1} \ldots (x - \alpha_r)^{m_r} = f = \gamma(f) = (x - \alpha_2)^{m_1} (x - \gamma(\alpha_2))^{m_2} \ldots (x - \gamma(\alpha_r))^{m_r}.
\]

As the power of \((x - \alpha_2)\) is the same in each expansion of \(f\) we must have that \(m_1 = m_2\) since \(\gamma\) is bijective and \(k[x]\) is a UFD. \(\square\)

**Note:** If \(\text{char}(k) = p > 0\), then \(p\) divides the multiplicity of each root (and they’re all the same by the corollary). In fact, each multiplicity must be a power of \(p\). We’ll show that now: Let \(f\) be a monic, irreducible polynomial in \(k[x]\). Then over \(k^a[x]\), \(f\) factors as \(f(x) = (x - \alpha_1)^m \ldots (x - \alpha_r)^m\) by the above corollary. Now, Let \(m = p^n\)

\(^{53}\)The correct word is not productands...idiot!

\(^{54}\)This is because fields have no nontrivial ideals, the kernel must be an ideal, and not everything can be mapped to 0.

\(^{55}\)This means that we never need to show that field homomorphisms are injective on the homework (or Friday night activities)! Ever!

\(^{56}\)Monic just makes the proof easier, but isn’t necessary!
where \( p \nmid n \). Then using the fact that the Frobenius map is in fact a homomorphism we get

\[
\begin{align*}
f(x) &= \left((x - \alpha_1) \cdot \ldots \cdot (x - \alpha_r)\right)^n \\
&= \left((x^{p^n} - \alpha_1^{p^n}) \cdot \ldots \cdot (x^{p^n} - \alpha_r^{p^n})\right)^n \\
&= g(x^{p^n})
\end{align*}
\]

where \( g \) is some polynomial in \( k[x] \). Moreover, \( g \) is irreducible with roots \( \alpha_i^{p^n} \) for each \( i \). Since \( g(x) = \left((x - \alpha_1^{p^n}) \cdot \ldots \cdot (x - \alpha_r^{p^n})\right)^n \) then if \( n > 1 \) we get that \( g \) is irreducible with multiple roots, but \( p \nmid n \) which is a contradiction, and so we must have \( n = 1 \) so that \( m = p^n \).

\> **Corollary:** Let \( f \in k[x] \) be irreducible with a field of characteristic \( p > 0 \). Then there exists an \( s \geq 0 \) such that \( f(x) = g(x^s) \) and \( g \) is an irreducible, separable polynomial.

\> **Corollary:** Let \( \alpha \) be algebraic over a field \( k \), with char \( k = p > 0 \). Then \( \alpha^{p^n} \) is separable for some \( s \geq 0 \).

\> **Fact:** Let \( k \subseteq K \) be a field extension, and let \( \alpha_1, \ldots, \alpha_r \in K \) be algebraic and separable over \( k \). Then \( E = k(\alpha_1, \ldots, \alpha_r) \) is a separable extension of \( k \).

**Proof.** Let \( \beta \in E \) and assume that \( \beta \) is not separable over \( k \). Then \( [k(\beta) : k] < [k(\beta) : k] \). Thus, \( [E : k]_s = [E : k(\beta)]_s \cdot [k(\beta) : k] = [E : k] \). However, we also have that because simple algebraic extensions are separable, then

\[
[E : k]_s = [E : k(\alpha_1, \ldots, \alpha_{r-1})]_s \ldots [k(\alpha_1) : k]_s
\]

is an intermediate field \( k \subseteq E \subseteq K \).

This is a contradiction, and so we must have that \( \beta \) is separable over \( k \).

\[\square\]

**14 November 2011**

\> **Theorem of the Primitive Element**

\> **Corollary:** Let \( k \subseteq K \) be an algebraic extension of fields. Also, let \( E = \{\alpha \in K : \alpha \) is separable over \( k \} \). Then \( E \) is an intermediate field \( k \subseteq E \subseteq K \).

**Proof.** It is enough to show that \( k(E) = E \). It is clear that \( E \subseteq k(E) \), so let \( \beta \in k(E) \). Then there exist \( \alpha_1, \ldots, \alpha_r \in E \) such that \( \beta \in k(\alpha_1, \ldots, \alpha_r) \subseteq k(\alpha) \). But we saw last time that \( k(\alpha_1, \ldots, \alpha_r) \) is separable over \( k \).

Thus, \( \beta \) is separable over \( k \) and so \( \beta \in E \).

\[\square\]

\> **Definition:** Let \( k \subseteq F \) be an algebraic extension of fields, and let \( E = \{\alpha \in F : \alpha \) is separable over \( k \} \). Then we call \( E \) the \textit{separable closure of} \( k \) \textit{in} \( F \).

\> **Comment:** If \( F \neq E \) in the above definition, then char \( k = p > 0 \), and for each \( \beta \in F \), there is an \( n \) (which depends on \( \beta \)) so that \( \beta^{p^n} \in E \). This is because \( \text{Irr}(\beta, k, x) = f(x^{p^n}) \) where \( f \) is separable. Moreover, \( \text{Irr}(\beta, k, x) \) divides \( x^n - \beta^{p^n} = (x - \beta)^m \) and so we have that \( \text{Irr}(\beta, k, x) \) is purely inseparable if for each element \( \beta \in F \) there is an \( n \) such that \( \beta^{p^n} \in k \).

\> **Definition:** We say an algebraic extension \( k \subseteq F \) (where char \( k = p > 0 \)) is \textit{purely inseparable} if for each element \( \beta \in F \) there is an \( n \) such that \( \beta^{p^n} \in k \). If \( k = F \), then regardless of characteristic, we also say \( F \) is a purely inseparable extension of \( k \).

\> **Corollary:** Let \( k \subseteq F \) be an algebraic extension field. Let \( E \) be the separable closure of \( k \) \textit{in} \( F \). Then \( k \subseteq E \) is separable and \( E \subseteq F \) is purely inseparable.

\> **Definition:** We say an extension \( k \subseteq F \) is \textit{simple} if there is an \( \alpha \in F \) such that \( k(\alpha) = F \). If \( k(\alpha) = F \), we say that \( \alpha \) is a \textit{primitive element}.

\> **Theorem of the Primitive Element:** Let \( k \subseteq E \) be a finite extension of fields.

1. If \( E \) is separable over \( k \), then \( E \) is a simple extension, that is, there is an element \( \delta \in E \) such that \( E = k(\delta) \).
2. The extension is simple if and only if there are only finitely many intermediate fields.

**Proof.** 1. First, suppose that \( |E| < \infty \). Then \( E \) is also a finite field. But \( E^* = E \setminus \{0\} \) is a cyclic group (under multiplication), so let \( E^* = \langle \alpha \rangle \). Then we get \( E = k(\alpha) \). Next, suppose that \( k \) is an infinite field. It is enough to show that \( k(\alpha, \beta) = k(\delta) \) for some \( \delta \in k(\alpha, \beta) \). Let \( \sigma_1, \ldots, \sigma_n \) be the distinct \( k \)–homomorphisms of \( E \to k^a \). Note \( n = [E : k]_s = [E : k] \). So consider the polynomial

\[
P(x) = \prod_{i \neq j} (\sigma_i(\alpha) + \sigma_i(\beta)x - (\sigma_j(\alpha) + \sigma_j(\beta)x)).
\]
In particular, since \( \sigma_i \neq \sigma_j \), then we have that \( P(x) \neq 0 \). Since \( |k| = \infty \), we can find a \( c \in k \) so that \( P(c) \neq 0 \). Thus, \( \sigma_i(\alpha) + \sigma_j(\beta)c \) is different for all \( i = 1, \ldots, n \). Thus, \( \sigma_i|_{k(\alpha + \beta)c} \) is different for each \( i = 1, \ldots, n \). Thus, \( [k(\alpha + \beta)c : k] \geq n \). This gives then that \( n \leq [k(\alpha + \beta)c : k] = [k(\alpha + \beta)c : k] \leq [k(\alpha, \beta) : k] = n \). Hence, \( k(\alpha + \beta)c = k(\alpha, \beta) \).

2. First, suppose that \( |k| < \infty \). Then for any finite extension \( k \subseteq E \), we have that \( |E| < \infty \) as well, and \( k \subseteq E \) is simple, and so there are only finitely many intermediate fields. Next, suppose that \( k \) is an infinite field. We’ll start by assuming there are finitely many intermediate fields and showing that the extension is simple. Again, it is enough to show that for \( \alpha, \beta \in K \) that \( k(\alpha, \beta) \) is actually a simple extension. So there exist \( c_1, c_2 \in k \) so that \( c_1 \neq c_2 \neq 0 \) and \( k(\alpha + c_1 \beta) = k(\alpha + c_2 \beta) \). This gives that \( (c_1 - c_2) \beta = (\alpha + c_1 \beta) - (\alpha + c_2 \beta) \in k(\alpha + c_2 \beta) \). Thus, \( \beta \in k(\alpha + c_2 \beta) \). Now using the fact that \( \beta \in k(\alpha + c_2 \beta) \), we get that \( \alpha = \alpha + c_2 \beta - c_2 \beta \in k(\alpha + c_2 \beta) \). Thus, \( k(\alpha, \beta) \subseteq k(\alpha + c_2 \beta) \subseteq k(\alpha, \beta) \) and hence \( k(\alpha + c_2 \beta) = k(\alpha, \beta) \).

Now, assume \( k \subseteq E \) is a simple extension. In particular, let \( E = k(\delta) \) for some \( \delta \in k^a = E^a \). Our goal is to show that there are only finitely many intermediate fields between \( k \) and \( E \). We’ll show there is an injection from the set of intermediate fields to the set of monic factors of \( f = \text{Irr}(\delta, k, x) \). Since the monic factors is clearly a finite set, then the other set will be finite as well, and that will complete the proof. So let \( F \) be an intermediate field, i.e. \( k \subset F \subseteq E \). Then \( F(\delta) = E \). So consider \( g_F(x) = \text{Irr}(\delta, F, x) \). Then clearly \( g_F|F \).

We’re now ready to define a map

\[
\varphi : \{\text{intermediate fields}\} \rightarrow \{\text{monic factors of } f\}
\]

by setting \( \varphi(F) = g_F \). Instead of directly showing that \( \varphi \) is injective, we’ll actually show that we can recover \( F \) from \( g_F \). Let \( K_{g_F} = k(a_1, \ldots, a_m) \) where \( g_F = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_0 \). It is clear that \( K_{g_F} \subseteq F \) as each \( a_i \in F \). So we must show the other inclusion. We’ll do this by looking at degrees. It is clear that \( |E : F| = |F(\delta) : F| = \deg g_F \) as \( E = F(\delta) \) and by the definition of \( g_F \). Similarly, it is clear that \( |E : K_{g_F}| = \deg(\text{Irr}(\delta, K_{g_F}, x)) = \deg(g_F|E) \) since \( E = K_{g_F}(\delta) \) and \( \text{Irr}(\delta, K_{g_F}, x) = g_F \). Thus, we have \( |E : F| = |E : K_{g_F}| = |E : F| \cdot |F : K_{g_F}| \) so that \( |F : K_{g_F}| = 1 \) and hence \( F = K_{g_F} \) so that there is an inverse map, an hence \( \varphi \) is injective (and hence completing the proof).

\[\Box\]

16 November 2011

Proof Completion

▷ Today was short and we just finished the proof that I’ve put completely above for the sake of simplicity.

18 November 2011

None

21 November 2011

Separable Degree & Galois Theory

▷ RECALL: Let \( k \subseteq F \) be fields, and assume the extension is algebraic. Then we have \( k \subseteq E \subseteq F \) where \( E := \{\alpha \in F : \alpha \text{ is separable}\} \) and \( E \subseteq F \) is purely inseparable.

▷ RECALL: If \( k \subseteq F \) is a finite extension and \( E \) is the separable closure of \( k \) in \( F \), then

\[
[F : k] = [F : E] \cdot [E : k],
\]

\[
[F : k]_s = [F : E]_s \cdot [E : k]_s, \text{ and}
\]

\[
[F : k]_i = [F : E]_i \cdot [E : k]_i
\]

since each type of degree is multiplicative (i.e. this holds for any intermediate field \( k \subseteq E \subseteq F \)).

▷ PROPOSITION: Let \( k \subseteq F \) be a finite field extension, and let \( E \) be the separable closure of \( k \) in \( F \). Then \( [E : k]_s = [E : k] = [F : k]_s = [F : E]_s = 1, [F : E] = [F : E], \) and \( [E : k]_i = 1 \).

Proof. We’ll start by showing that \( [E : k]_s = [E : k] \). By the theorem of the primitive element, there is an \( \alpha \in E \) such that \( E = k(\alpha) \) (since \( E \) is a separable extension of \( k \)). However, \( [E : k] = \deg(\text{Irr}(\alpha, k, x)) \) and \( \text{Irr}(\alpha, k, x) \) is separable. For each root, \( \beta \) of \( \text{Irr}(\alpha, k, x) \) we get a \( k \)–homomorphism \( k(\alpha) \rightarrow k^a \) given by \( \alpha \mapsto \beta \). Thus, the number of \( k \)–homomorphisms \( k(\alpha) \rightarrow k^a \) is at least the number of distinct roots of \( \text{Irr}(\alpha, k, x) \), but that’s equal to \( \deg \text{Irr}(\alpha, k, x) = [E : k] \) since \( \alpha \) is separable. Hence, \( [E : k]_s \geq [E : k] \geq [E : k]_s \) and so we get that \( [E : k]_s = [E : k] \). Next, we’ll show that \( [F : E]_s = 1 \). Once we’ve shown that, then we get \( [F : k]_s = [F : E]_s \cdot [E : k]_s = [F : E]_s \cdot [E : k] = [E : k] \). So, let \( \sigma \) be an \( E \)–homomorphism \( \sigma : F \rightarrow E^a \) and \( \sigma : F \rightarrow F^a \). Thus, \( \sigma|_E = \text{id}_E \). Let \( \beta \in F \). If \( \text{char}(E) = 0 \), then \( F \) is automatically a separable extension of \( k \) so that \( F = E \) and \( \sigma(\beta) = \beta \). However, if \( \text{char}(E) = p > 0 \), then

\[\text{This is because the polynomial can have only finitely many roots.}\]
We now claim that $\text{Aut}(\mathbb{Q}(\sqrt{2})) = \{1, \sqrt{2}\}$. It is clear that $\alpha : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ be a $\mathbb{Q}$-homomorphism. Then we can extend this to a $\mathbb{Q}$-homomorphism $\bar{\alpha} : \mathbb{Q} \to \mathbb{Q}$. Here $\bar{\alpha}$ permutes the roots of $\text{Irr}(\sqrt{2}, \mathbb{Q}, x) = x^3 - 2$. However, $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ and so $\mathbb{Q}(\sqrt{2})$ contains only one root of $x^3 - 2$. Thus, $\sigma(\sqrt{2}) = \sqrt{2}$ so that $\sigma = 1_{\mathbb{Q}(\sqrt{2})}$ and hence $\text{Gal}(\mathbb{Q}) = \{1, \sqrt{2}\}$.

**28 November 2011**

**Definition:** Let $k \subseteq K$ be an algebraic extension of fields. We say it is a Galois extension if it is normal and separable.

**Fundamental Theorem of Galois Theory:** Let $k \subseteq K$ be a finite Galois extension of fields. Then $F$ and $G$ give a bijection from the set of intermediate fields $k \subseteq E \subseteq K$ to the set of subgroups of $\text{Aut}_k(K)$. Moreover, an intermediate field $E$ is Galois over $k$ if and only if $\text{Aut}_E(K) \leq \text{Aut}_k(K)$, and in this case, $\text{Aut}_E(K) \cong \	ext{Aut}_k(K)/\text{Aut}_E(K)$.

**Artin’s Theorem:** Let $K$ be any field, and let $G$ be a finite subgroup of $\text{Aut}(K)$. Let $k = K^G$. Then $k \subseteq K$ is a finite Galois extension with Galois group $G = \text{Aut}_k(K)$ and $|K : k| = |G|$.

*Proof.* We start by claiming that $k \subseteq K$ is separable. So let $\alpha \in K$. It is enough to show that $f(\alpha) = 0$ for some polynomial $f \in k[x]$ which does not have multiple roots. So let $\{\alpha_1, \ldots, \alpha_r\} = G$ be the orbit of $\alpha$ under the action of $G$. Also, do this so that $\alpha_i \neq \alpha_j$ whenever $i \neq j$. Then set $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r)$. Note here that $f \in k[x]$, and that $G$ acts on $K$, so that we have an action of $G$ on $K[x]$. In particular, if $g \in G$, then $g \cdot f = (x - g(\alpha_1))(x - g(\alpha_2)) \cdots (x - g(\alpha_r)).$ But we know that $\{g(\alpha_1), \ldots, g(\alpha_r)\} = \{\alpha_1, \ldots, \alpha_r\}$ since $G$ just permutes the elements of an orbit. Thus, $g \cdot f = f$. Hence the coefficients of $f$ as a (non-factored) polynomial are fixed by the action of $G$, and so they’re elements of $k$ and $f \in k[x]$. But $f$ is separably by construction, and so $k \subseteq K$ is separable and algebraic.

We now claim that $k \subseteq K$ is a normal extension. Let $\alpha \in K$ and let $f_\alpha$ be the $f$ as defined in the previous part. Note that $f_\alpha$ splits over $K$ and the roots are all in $K$. Thus, $K$ is the splitting field of $\{f_\alpha : \alpha \in K\}$. Thus, $k \subseteq K$ is Galois and $G \leq \text{Aut}_K(K)$.

Now, if $[K : k] < \infty$, then $K^G = k$, and of course $K^{\text{Aut}_K(K)} = k$. Thus, under the Galois bijection, both $G$ and $\text{Aut}_k(K)$ correspond to $K$. Then, by the usual statement of the Fundamental Theorem of Galois Theory, we have that $|G| = |\text{Aut}_k(K)| = [K : k]$. So consider the case when $[K : k] = \infty$. Then there must be an intermediate field $k \subseteq E \subseteq K$ so that $|G| = [E : k] < \infty$. By choosing such an intermediate field $E$, we know that $E$ will be a finite extension of $k$. Then the theorem of the primitive element says that $E = k(\gamma)$ for some $\gamma \in E$. Now, we claim that $f_\gamma = \text{Irr}(\gamma, k)$ is separable.

It is clear that $f_\gamma \in k[x]$ from our previous reasoning, and that $f_\gamma(\gamma) = 0$ by definition. So thus, we get that $f_\gamma(\gamma, k, x) = \text{Irr}(\gamma, k, x)$. On the other hand, the group $\text{Aut}_k(K)$ acts transitively on the roots of $f_\gamma$, but preserves the set of roots of $\text{Irr}(\gamma, k, x)$. Since $g \cdot \text{Irr}(\gamma, k, x) = \text{Irr}(\gamma, k, x)$ for all $g \in \text{Aut}_k(K)$, we see that if $\delta$ is a root of $\text{Irr}(\gamma, k, x)$ then so is $g \cdot \delta$ for all $g \in \text{Aut}_k(K)$. Thus, the set of roots of $\text{Irr}(\gamma, k, x)$ is exactly $\text{Aut}_k(K) \cdot \gamma$ and so contains $G \cdot \gamma$. Since $\text{Irr}(\gamma, k, x) \subseteq _g f_\gamma$, then we get the other inclusion, and so the sets of roots are equal, and hence $f_\gamma = \text{Irr}(\gamma, k, x)$ as they’re both monic and separable.

Now, we have $|G| \geq t = \deg \text{Irr}(\gamma, k, x) = [k(\gamma) : k] = [E : k] > |G|$. This is a contradiction, and so we can’t ever have that $[K : k] = \infty$, and that completes the proof.

---

58 We defined these functors on 21 November 2011.

59 This can be done by adding elements one at a time until you get that the index is sufficiently large.
30 November 2011

Galois Extensions & Finite Fields

Aside: If \( k \subseteq K \) is a Galois extension, then \( |\text{Aut}_k(K)| = [K : k] \).

Aside: Here, we see how to get extensions \( k \subseteq K \) with any Galois group, as long as \( G \leq \text{Aut}(K) \).

Noether’s Problem: What groups occur as Galois groups of finite Galois extensions of \( \mathbb{Q} \)?

In conclusion: If \( F/k \) is finite, we have

\[
|\text{Aut}_k(F)| \leq |F : k|_s \leq |F : k|
\]

where if the extension is normal then the first is an equality and if it is also Galois, then they’re both equalities. (i.e. the first is an equality when the extension is normal and the second is an equality when the extension is separable).

Finite Fields: Let \( K \) be a finite field, and set \( p = \text{char}(K) > 0 \). Note that \( |K| = p^n \) for some \( n \geq 1 \). Also, let \( k \) be the prime field, so \( k \cong \mathbb{Z}/p\mathbb{Z} \). Thus, \( |K : k| = n \). We have the Frobenius automorphism, which we’ll call \( \varphi \) that sends elements of \( K \) to their \( p \)-th powers. In particular if \( \alpha \in k \) then \( \varphi(\alpha) = \alpha^p = \alpha \) so that \( \varphi \in \text{Aut}_k(K) \).

Claim: \( \text{Aut}_k(K) \) is a cyclic group generated by the Frobenius map \( \varphi \) for any finite field \( K \) where \( k \) is the prime field, and hence isomorphic to \( \mathbb{Z}/p\mathbb{Z} \) for some prime \( p \).

Proof. It is enough to show that the order of \( \varphi \) is \( n \). So recall that \( K^* \) is a cyclic group under multiplication, and let \( K^* = (\alpha) \). But the order of \( \varphi \) is the least \( m \geq 1 \) such that \( \varphi^m(\alpha) = \alpha \). However, the number of roots of \( x^{p^n} - \beta \) is at most \( p^n \) so the order of \( \varphi \) is at least \( n \) since we need \( p^n \) roots to get all elements of \( K \) as roots of the polynomial \( x^{p^n} - \beta \). On the other hand, the order of \( \alpha \) in \( K^* \) is \( p^n - 1 \). So \( \varphi^{n^{-1}} = 1 \) and so \( \alpha^{p^n-1} = \alpha \). Hence, \( \varphi^n(\alpha) = \alpha \) so that \( \varphi^n(\alpha^i) = \alpha^i \) for all \( i \). Since \( \alpha \) generates \( K^* \) then \( \varphi^n(\alpha^i) = \alpha^i \) for all \( \beta \neq 0 \) and so \( \varphi^n(\beta) = \beta \) for all \( \beta \in K \). Thus, \( n \) is the order of \( \varphi \).

Comment: If \( k \subseteq E \subseteq K \), then \( \text{Aut}_k(K) \supseteq \text{Aut}_E(K) \), so \( \text{Aut}_E(K) \) is generated by a power of \( \varphi \).

2 December 2011

Finite Fields

Last Time: We saw that if \( F \) is a finite field with prime field \( k = \mathbb{Z}/p\mathbb{Z} \), then \( \text{Aut}_k(K) = (\varphi) \) where \( \varphi \) is the Frobenius homomorphism. If \( |F| = p^n \) for some \( n \geq 1 \) then the order of \( \varphi \) is \( n \).

Note: If \( F_1 \) and \( F_2 \) are finite fields with \( |F_1| = |F_2| \), then \( F_1 \cong F_2 \).

Galois Correspondence for Finite Fields: Say \( k \) is the prime field, and \( F \) is an extension field with \( |F| = p^n \). Consider an intermediate field \( k \subseteq E \subseteq F \). Then these correspond to (respectively)

\[
\text{Aut}_k(F) \supseteq \text{Aut}_E(F) \supseteq \text{Aut}_F(F) = \{\text{id}_F\}.
\]

Here, \( |k| = p \), \( |F| = p^n \) and \( n = |F : k| = |F : E| |E : k| \) so if we let \( |F : E| = r \) and \( |E : k| = s \), then \( n = rs \), and \( |E| = p^r \). Let \( \varphi_F \) be the Frobenius map on the field \( F \). As a vector space \( E \cong k^s \). Also \( \text{Aut}_k(E) \) is a cyclic group of order \( s \), and \( \text{Aut}_k(E) \cong \text{Aut}_k(F)/\text{Aut}_k(E) \). Since \( |\text{Aut}_E(F)| = |F : E| = r \), it is clear that \( \text{Aut}_F(F) \) is a group of order \( r \) but it is not clear which group of order \( r \) it is. Since \( |\text{Aut}_k(F)| = n \) and \( \text{Aut}_k(F) = (\varphi_F) \) and \( |\text{Aut}_F(F)| = r \), then \( \text{Aut}_F(F) = (\varphi_F^k) \). Thus, we have \( k \subseteq E \subseteq F \) correspond to \( (\varphi_F^k) \supseteq (\varphi_F^E) \supseteq (\varphi_F^{kE}) = (1_F) \) respectively.

60This problem is still open and interesting.

61This is sufficient because we know that the group has order \( n = |K : k| = |\text{Aut}_k(K)| \) so if it has an element of order \( n \) then it will be cyclic of order \( n \).
Example(s):
- For every integer \( n \geq 1 \), there is a finite field, \( F \) of order \( p^n \) where \( p \) is any prime. Namely, \( F \) is the splitting field for \( x^{p^n} - x \) over \( k = \mathbb{Z}/p\mathbb{Z} \). If \( n \) is prime, then the only intermediate fields are \( F \) and \( k \). (Due to the Galois correspondence!)
- Let \( p = 31991 \). Note that this is prime. (We could use any other prime, but this one is large enough to be awkward to raise to powers, and yet still relatively small in computer terms). We want to find all intermediate \( K \) fields of the form \( k \subset \mathbb{Q} \leq K \) for \( n \) when \( k = \mathbb{Z}/p\mathbb{Z} \) and \( |F| = p^n \). First, we’ll find the lattice of subgroups of the cyclic subgroup of order 12. For notational simplicity, we’ll denote the cyclic group of order \( n \) by \( C_n \):

Thus, there are 6 intermediate fields, and their lattice is the same as for the lattice of subgroups, except the bigger fields are at the top, rather than at the bottom of the picture.
- How many elements of \( F \) generate \( F \) over \( k \) if \( F \) and \( k \) are fields, \( p \) is prime, \( |k| = p \) and \( |F| = p^6 \)? Here, the goal is to count all \( \alpha \in F \) so that \( k(\alpha) = F \). We have the following lattice of subfields, where \( \widetilde{C}_n \) is the subfield corresponding to the cyclic group of order \( n \):

Let \( S = F \setminus (\widetilde{C}_2 \cup \widetilde{C}_3) \). Then we want to count the size of \( S \).\(^{63}\) So, \(|S| = |F| - (|\widetilde{C}_2| + |\widetilde{C}_3|) + |\widetilde{C}_6| = p^6 - p^2 - p^3 + p.\)

5 December 2011

Definition: Let \( k \subseteq K \) be fields, and \( S \) a subset of \( K \). We say that the elements of \( S \) are algebraically independent over \( k \) if for any \( r \) and any subset \( \{s_1, \ldots, s_r\} \subseteq S \) of \( r \) distinct elements, the \( k \)-homomorphism \( \varphi : k[x_1, \ldots, x_r] \to K \) given by \( x_i \mapsto s_i \) is injective.

Note: If \( \{s_1, \ldots, s_r\} \subseteq K \) is algebraically independent over \( k \), then \( k(x_1, \ldots, x_r) \cong k(s_1, \ldots, s_r) \) and the isomorphism can be given by \( x_i \mapsto s_i \), which is a \( k \)-homomorphism.

Definition: If \( S \subseteq K \) is algebraically independent over \( k \) for some subfield \( k \subseteq K \), and if \( K = k(S) \), then we say that \( k \subseteq K \) is a purely transcendental extension.

Example: Let \( k = \mathbb{Q} \), and \( K = \mathbb{Q}(x) \). Then \( k \subseteq K \) is a purely transcendental extension (this is easily seen by using the set \( S = \{x\} \)). However, \( x^2 \in K \), and so \( \mathbb{Q} \subseteq \mathbb{Q}(x^2) \subseteq \mathbb{Q}(x) \) so with respect to the set \( T = \{x^2\} \) (which is also an algebraically independent set), it appears as if the extension is not purely transcendental since we get that \( k(T) \subseteq K \).

Definition: Let \( k \subseteq K \) be fields. Partially order the set of subsets \( S \subseteq K \) which are algebraically independent over \( k \) by inclusion. We say a subset \( B \subseteq K \) which is algebraically independent over \( k \) is a transcendence base if \( B \) is not properly contained in any other subset \( S \subseteq K \) which is algebraically independent over \( k \).

Example: Let \( k = \mathbb{Q} \), \( K = \mathbb{Q}(x) \). Then \( \{x\} \) is a transcendence base for \( k \subseteq K \). Also, \( \{x^2\} \) is a transcendence base for the extension even though \( k(x^2) \nsubseteq K \).

Note: If \( S \) is a transcendence base for \( k \subseteq K \), then \( k(S) \subseteq K \) is an algebraic extension.

Comment: Sometimes it is impossible to pick a transcendence base \( S \) for a field extension \( k \subseteq K \) such that \( k(S) = K \).

Example: For example, \( \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \) is an algebraic extension and so its transcendence base is the empty-set. Also, \( \mathbb{Q} \subseteq \mathbb{Q}(\pi, \sqrt{2}) \) is probably not purely transcendental.

\(^{63}\) This will be done using inclusion exclusion.
7 December 2011

**Theorem:** Let $k \subseteq K$ be fields. Then there is a transcendence base for this extension.\(^{64}\)

**Key Lemma:** Let $k \subseteq K$ be fields. Let $S \subseteq K$ be algebraically independent over $k$. Let $u \in K$. Then $T = S \cup \{ u \}$ is algebraically independent over $k$ if and only if $u$ is transcendental over $k(S)$.

**Proof.** We’ll prove this next time, but first state some corollaries now.

**Corollary 1:** Let $k \subseteq K$ be fields, with $S \subseteq K$ an algebraically independent set over $k$. Then $S$ is a transcendence base for $k \subseteq K$ if and only if $k(S) \subseteq K$ is algebraic.

**Corollary 2:** Let $S_1$ and $S_2$ be transcendence bases for $k \subseteq K$. If $|S_1| < \infty$, then $|S_2| < \infty$ and $|S_1| = |S_2|$.\(^{65}\)

**Definition:** We define the **transcendence degree** of $k \subseteq K$, denoted $\operatorname{trdeg}_k(K)$ to be $|S|$ where $S$ is a transcendence basis for $k \subseteq K$.

---

**Transcendence Bases**

**Corollary 3:** Let $k \subseteq K$ be fields, and let $S \subseteq K$ be a subset. If $K$ is algebraic over $k(S)$, then $S$ contains a transcendence base for $k \subseteq K$.

**Corollary 4:** Let $k \subseteq K$ be fields. Let $S \subseteq K$ be algebraically independent over $k$. Then there is a transcendence base $S'$ for $k \subseteq K$ so that $S \subseteq S'$.

**Corollary 5:** Let $k \subseteq K \subseteq L$ be fields. Then $\operatorname{trdeg}_k(K) + \operatorname{trdeg}_K(L) = \operatorname{trdeg}_K(L)$.

**Note:** We’re now ready to prove things:

- **Proof.** Of Key Lemma: ($\Rightarrow$) We’ll prove this direction by contrapositive. So we’re assuming that $u$ is algebraic (i.e. not transcendental) over $k(S)$ and we need to show that $T = S \cup \{ u \}$ is not algebraically independent over $k$. So let $f = \operatorname{Irr}(u,k(S),x)$ and write it as $f(x) = \sum_{i=0}^{d} \frac{g_i}{h_i} x^i$ where $g_i = \tilde{g}_i(s_1,\ldots,s_r)$ and $h_i = \tilde{h}_i(s_1,\ldots,s_r) \neq 0$ where $\tilde{g}_i,\tilde{h}_i \in k[x_1,\ldots,x_r]$ for some $r \in \mathbb{N}$ and $s_1,\ldots,s_r \in S$. Then, let $\tilde{f} = \sum_{i=0}^{d} \frac{\tilde{g}_i}{\tilde{h}_i} x^i$ and note that $\tilde{f} \in (x_1,\ldots,x_r)$. Let $\tilde{H} = \tilde{h}_0 \cdot \tilde{h}_1 \cdots \tilde{h}_d$. Then $\tilde{H} \tilde{f}$ is a polynomial, which we’ll call $\tilde{F}$. Then $\tilde{F}(s_1,\ldots,s_r,u) = \tilde{H}(s_1,\ldots,s_r)\tilde{f}(s_1,\ldots,s_r,u) = \tilde{H}(s_1,\ldots,s_r)f(u) = 0$ as $f(u) = 0$. So $\tilde{F} \in \ker \varphi$ where $\varphi: k[x_1,\ldots,x_r] \to K$ is given by $x_i \mapsto s_i$ and $x \mapsto u$. But $F$ is not the zero polynomial since $f \neq 0$, so that $\tilde{f} \neq 0$, and each $\tilde{h}_i \neq 0$ so each $h_i \neq 0$. Thus, $\tilde{H} \neq 0$, and so $\tilde{F} \neq 0$. This means that $\ker \varphi \neq 0$ and so $T$ is not algebraically independent.

($\Leftarrow$) Now, we’ll assume that $u$ is transcendental over $k(S)$ and we need to show that $T = S \cup \{ u \}$ is algebraically independent over $k$. Let $t_1,\ldots,t_r \in T$. If $t_i \neq u$ for any $i$, then $t_i \in S$ for all $i$ and hence $t_1,\ldots,t_r$ are algebraically independent, so that $k[x_1,\ldots,x_r] \to K$ given by $x_i \mapsto t_i$ is injective. So instead suppose that $t_i = u$ for some $i$. Without loss of generality, we may assume $u = t_r$. Then $\varphi: k[x_1,\ldots,x_{r-1}] \to K$ given by $x_i \mapsto t_i$ for $i < r$ and $x_r \mapsto u = t_r$ can be written as the composition of two maps. Namely, $\varphi_1: k[x_1,\ldots,x_r] \to k(S)[x_r]$ given by $x_i \mapsto t_i$ for $i < r$ and $x_r \mapsto x_r$ and $\varphi_2: (k(S)[x_r] \to K$ given by $x_r \mapsto u$. Then $\varphi_1$ is injective as $t_1,\ldots,t_{r-1}$ are algebraically independent over $k$ and $\varphi_2$ is injective as $u$ is transcendental over $k(S)$. Thus, $\varphi = \varphi_2 \circ \varphi_1$ is injective, so that $T$ is algebraically independent over $k$.

**Aside:** If $t_1,\ldots,t_r \in S$ and $S$ is algebraically independent over $k$, then $k[x_1,\ldots,x_{r-1}] \to k(S)$ is injective where $x_i \mapsto t_i$. So in the proof of the Key Lemma we use the easy fact that $k[x_1,\ldots,x_{r-1}][x_r] \to k(S)[x_r]$ is also injective.

**Comment:** The empty-set is always algebraically independent.

**Comment:** Any subset of an algebraically independent set is also algebraically independent.

**Comment:** If $\alpha \in S$ with $S$ a subset of $k$ and $k \subseteq K$ a subfield, then if $S$ is algebraically independent over $k$, we must also have that $\alpha$ is transcendental over $k$.

**Note:** We didn’t prove the remaining Corollaries in class, but they’re not terribly difficult so I’ll include them here.

- **Proof.** Of Corollary 2: First suppose $S_1 = \emptyset$. Then $k(S_1) = k$ so that $K/k$ is an algebraic extension. Thus, $K$ has no elements that are transcendental over $k$ and hence $S_2 = \emptyset$. In particular, this gives $|S_2| < \infty$ and $|S_1| = |S_2|$.

So now suppose that $S_1 = \{ s_1,\ldots,s_r \}$ with $s_i \neq s_j$ if $i \neq j$, for some $r \geq 1$. Then $K/k(s_2,\ldots,s_r)$ is not algebraic since $s_1$ is transcendental over $k(s_2,\ldots,s_r)$. Thus, there is a transcendental element in $S_2$, since

---

\(^{64}\)The proof is just a simple application of Zorn's lemma.

\(^{65}\)It is true in general that they have the same cardinality, but that’s significantly harder to prove, and requires transfinite induction...ick!
9 December 2011

HILBERT & RINGS OF INVARIANTS: Let G be a group, acting as k–automorphism on \( R = k[x_1, \ldots, x_n] \) where k is a field. The big question here is whether the ring of invariants, \( R^G \) is always finitely generated over k. Hilbert proved that the answer is yes for certain groups, called reductive groups. The key idea in the proof was that if \( R \) is Noetherian! Hilbert’s 14th problem was asking if the ring of invariants is always finitely generated. Zariski reformulated the problem in terms of an intermediate field, and Nagata found a counterexample. Apparently Rees was also instrumental in solving the problem, but we weren’t told how in class.

Fact: Let \( k \subseteq E \subseteq K \) be fields such that \( K = k(S) \) for some finite subset \( S \subseteq K \). Then \( E \) is finitely generated over \( k \).

Special Case: If \( k \subseteq E \subseteq K \) are fields and \( K \) is a purely transcendental extension of \( k \) with \( \text{trdeg}_k K < \infty \), and if \( E/k \) is algebraic, then it can be shown that \( E \) is finitely generated over \( k \).

\( k(s_2, \ldots, s_r)(S_2) = K \) is not algebraic over \( k(s_2, \ldots, s_r) \). So let \( \sigma_1 \in S_2 \) be transcendental over \( k(s_2, \ldots, s_r) \). We also get that \( s_1 \) is algebraic over \( k(\sigma_1, s_2, \ldots, s_r) \) since otherwise \( S_1 \) would not be a transcendence base. Thus, \( k(\sigma_1, s_1, \ldots, s_r) \) is algebraic over \( k(\sigma_1, s_2, \ldots, s_r) \), and since \( K \) is algebraic over \( k(\sigma_1, s_1, \ldots, s_r) \), then \( K \) is also algebraic over \( k(\sigma_1, s_2, \ldots, s_r) \), so that \( \{\sigma_1, s_2, \ldots, s_r\} \) is a transcendence base for the extension \( K/k \). By induction, we can replace all of the elements of \( S_1 \) with elements of \( S_2 \). If we run out of elements of \( S_1 \) to replace, or if we run out of elements of \( S_2 \) to replace elements of \( S_1 \) with, then we get a contradiction to one of the sets being a transcendence base. Thus, we must have that \( |S_1| = |S_2| \).

Proof of Corollary 3: Let \( \Sigma \) be a maximal algebraically independent subset of \( S \). Then \( K/k(\Sigma) \) is algebraic and \( k(S)/k(\Sigma) \) is algebraic, so that \( K/k(\Sigma) \) is algebraic. Thus, \( \Sigma \) is a transcendence base for \( K/k \) by the first corollary.

Proof of Corollary 4: Let \( \Sigma \) be a maximal algebraically independent subset of \( K \) which contains \( S \). Then \( K/k(\Sigma) \) is algebraic by the maximality, so that \( \Sigma \) is a transcendence base for \( K/k \) by corollary 1.

Proof of Corollary 5: Let \( S \) be a transcendence base for \( K/k \) and let \( T \) be a transcendence base for \( L/K \). Note that \( T \) is automatically algebraically independent over \( k \). If \( |S| = \infty \), then \( L/k \) has a transcendence base that contains \( S \). If \( |T| = \infty \), then \( L/k \) has a transcendence base that contains \( T \), and so if either \( S \) or \( T \) is an infinite set, then \( \text{trdeg}_k(L) = \infty \) and the statement holds.

So now we assume that both \( S \) and \( T \) are finite sets. Let \( S = \{s_1, \ldots, s_m\} \) and \( T = \{t_1, \ldots, t_n\} \). If \( S \cup T \) is not algebraically independent over \( k \), then there is a nonzero polynomial \( f \in k[x_1, \ldots, x_m, y_1, \ldots, y_n] \) such that \( f(s_1, \ldots, s_m, t_1, \ldots, t_n) = 0 \). Since \( f \in k[x_1, \ldots, x_m, y_1, \ldots, y_n] \subseteq k(S)[y_1, \ldots, y_n] \), and since \( T \) is algebraically independent over \( K \) (and hence over \( k(S) \)), then we have that \( f(s_1, \ldots, s_m, y_1, \ldots, y_n) \) is the zero element of \( k(S)[y_1, \ldots, y_n] \). However, since the original polynomial \( f \) was not the zero polynomial, then some monomial in the variables \( y_1, \ldots, y_n \) appears as a term in \( f \) with coefficient a nonzero element of \( k[x_1, \ldots, x_m] \), which when evaluated at \( s_1, \ldots, s_m \) gives zero. But this contradicts the fact that the set \( S \) is algebraically independent over \( k \), and hence \( S \cup T \) is algebraically independent over \( k \).

It remains to show that \( L \) is algebraic over \( k(S \cup T) \). However, we know that \( K \) is algebraic over \( k(S) \), so that \( K(T) \) is algebraic over \( k(S \cup T) \), and we also have that \( L \) is algebraic over \( K(T) \). Thus, \( L \) is algebraic over \( k(S \cup T) \), so that \( S \cup T \) is a transcendence base for \( L/k \) and hence we get the result:

\[
\text{trdeg}_k(K) + \text{trdeg}_K(L) = \text{trdeg}_k(L).
\]