Math 8000 (Graduate Algebra), Fall 2017

Asilata Bapat

Notes written collaboratively by the students and the instructor.

University of Georgia

August 15th, 2017 – December 5th, 2017

Contents

Part I: Group theory

1 Group theory fundamentals

1.1 *Review of groups*

Lecture 1
August 15th, 2017
Notes by Asilata Bapat

1.1 definition. A group is a triple (G, p, e) satisfying the following properties.

1. $p\colon G \times G \to G$ is an associative binary operation.
2. $e \in G$ is an *identity element*. That is, for every $g \in G$, we have $p(e, g) = p(g, e) = g$.
3. For every $g \in G$, there is some $h \in G$ such that $p(g, h) = p(h, g) = e$. Such an element is called an *inverse* of g.

It follows that every $g \in G$ has a unique inverse, which is denoted g^{-1}.

We usually write groups multiplicatively, where $p(g, h)$ is simply written as $g \cdot h$ or gh. In this case the identity element is sometimes called "1". If the binary operation is commutative, the group is called *abelian*. In this case it is more common to write it additively, so that $p(a, b)$ is written $a + b$, and the identity element is called "0". Structures satisfying only the first two conditions above are called monoids. Structures satisfying only the first condition above are called semigroups.

1.2 examples.

1. The additive group of the integers $(\mathbb{Z}, +, 0)$ is an abelian group.
2. $(\mathbb{N}, +, 0)$ is an abelian monoid.
3. The set of all permutations of $\{1, 2, \ldots, n\}$, under the operation of composing permutations, forms the *symmetric group* S_n. Its identity element is the identity permutation.
4. The set $GL_n(\mathbb{R})$ consisting of all $n \times n$ invertible matrices with real entries forms the *general linear group* under matrix multiplication. Its identity element is the $n \times n$ identity matrix.

Groups naturally arise as the set of bijective self-maps of some fixed set. That is, if S is any set, we can construct the following group $G(S)$:

$$G(S) = \{f\colon S \to S \mid f \text{ is bijective}\}.$$

The binary operation on this set is composition of functions. Namely if $f, g \in G(S)$, then fg is defined to be $f \circ g$ (remember, this means that you first

apply g, and then apply f). The identity element is the identity function. More generally, one could impose additional conditions to consider only a subset of the bijective self-maps of some fixed set.

For example, $S_n = G(\{1, 2, \ldots, n\})$, because a permutation is just a bijective self-map from $\{1, 2, \ldots, n\}$ to itself. On the other hand, $GL_n(\mathbb{R}) \subset G(\mathbb{R}^n)$. Recall that any $n \times n$ matrix gives a linear map of $\mathbb{R}^n$ to itself. So $GL_n(\mathbb{R})$ is the subset of $G(\mathbb{R}^n)$ consisting of bijective self-maps that are also linear.

More specifically, $GL_n(\mathbb{R})$ is a subgroup of $G(\mathbb{R}^n)$.

1.3 definition. A subset $H \subset G$ is a *subgroup* of G (denoted $H < G$) if the following conditions hold.

1. $e \in H$.
2. For every $h_1, h_2 \in H$ we have $h_1 h_2 \in H$.
3. For every $h \in H$ we have $h^{-1} \in H$.

1.4 remark. G is called a transformation group if there is some set S such that $G < G(S)$.

We now define group homomorphisms and isomorphisms.

1.5 definition. A function $\varphi\colon G \to H$ is called a *group homomorphism* if

1. for every $g_1, g_2 \in G$ we have $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$, and
2. if $\varphi(e_G) = e_H$.

It follows that for every $g \in G$, we have $\varphi(g^{-1}) = (\varphi(g))^{-1}$.

1.6 definition. A group homomorphism that is bijective is called a *group isomorphism*.

1.7 exercise. Check that if $\varphi\colon G \to H$ is an isomorphism of groups, then its inverse function $\psi\colon H \to G$ is also a group homomorphism.

1.8 example. The map $x \mapsto e^x$ is a group isomorphism from the additive group $(\mathbb{R}, +, 0)$ to the multiplicative group $(\mathbb{R}^{>0}, \cdot, 1)$.

Let us look at the example of the symmetric group in more detail. The group $S_2 = G(1, 2)$ has two elements. The first element is the identity element, and the second is the permutation that swaps the two numbers. If we let e be the identity element and σ the other element, then we can check that $\sigma^2 = e$, and that the group is abelian.

The group $S_3 = G(1, 2, 3)$ has six elements. For example, we have the permutation where $\{1 \mapsto 2,\ 2 \mapsto 1,\ 3 \mapsto 3\}$. A more concise way of writing this down is in the *cycle notation*. In cycle notation, we start a cycle at some

element, and follow it around the permutation until it comes back to itself. At this point we close the cycle and start a new one with a remaining element. For example, the element above is written as $(1\,2)(3)$ or simply as $(1\,2)$ (one-element cycles are often omitted). The identity element is usually written (1).

Another example of an element of S_3 in cycle notation is $(1\,3)$, which fixes 2 and swaps 1 with 3. The product $(1\,2)\cdot(1\,3)$ gives the permutation obtained by first applying $(1\,3)$ and then $(1\,2)$. We can check that this is $(1\,3\,2)$. On the other hand, the product in the reverse order $(1\,3)\cdot(1\,2)$ equals $(1\,2\,3)$. Notice that this example shows that S_3 is not abelian.

1.9 definition. The centralizer of an element $g \in G$, denoted $Z_g(G)$ or $C_g(G)$, is the set of all $h \in G$ such that $gh = hg$.

1.10 definition. The center of G, denoted $Z(G)$ or $C(G)$, is defined as

$$Z(G) = \bigcap_{g \in G} Z_g(G).$$

1.11 exercise. Check that $Z_g(G)$ and $Z(G)$ are subgroups of G.

Note that for any G, the subgroup $Z(G)$ is abelian.

1.12 exercise. Compute the centralizer of $(1\,2)$ in S_2, S_3, S_4 explicitly. Can you describe the centralizer of $(1\,2)$ in S_n for any n?

1.13 definition. Let $A \subset G$ be any subset (not necessarily a subgroup). The *subgroup generated by* A is defined to be the smallest subgroup of G that contains A as a subset.

"Smallest" means minimal with respect to inclusion.

Let us check that this is well-defined. More precisely, we must show that such an object exists, and that it is unique.

To show existence, define $H < G$ as follows:

$$H = \bigcap_{H' < G,\ H' \supset A} H'.$$

Clearly, $H \supset A$. To show that H is a subgroup, let h_1 and h_2 be any two elements of H. Then for any $H' < G$ that contains A, we have $h_1, h_2 \in H'$ and so $h_1 h_2 \in H'$. So $h_1 h_2$ lies in the intersection of all these H', which means that it lies in H. Similarly, one can check that the identity element lies in H, and that H is closed under inverses. Note that H cannot properly contain any subgroup of G that contains A, so we have proved the existence.

To show uniqueness, suppose that H_1 and H_2 are two smallest subgroups of G that contain A. Then it can be checked that $H_1 \cap H_2$ is another subgroup of G that contains A, which lies in both H_1 and H_2. Since H_1 and H_2 were both

smallest subgroups that contain A, it must be the case that $H_1 \cap H_2 = H_1$ and $H_1 \cap H_2 = H_2$, which means that $H_1 = H_2$.

As a particular case, if A is a set with one element, then the subgroup generated by A is called a *cyclic subgroup*.

1.14 examples. Let $G = GL_2(\mathbb{R})$. Let M be any matrix in G. Then the subgroup generated by the set $\{M\}$ is exactly the set $\{M^i \mid i \in \mathbb{Z}\}$.

1. If M is the matrix

$$\begin{pmatrix} 1 & 2 \\ 0 & -3 \end{pmatrix},$$

then the subgroup generated by M has infinite order (or cardinality).

2. If N is the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

then the subgroup generated by N has order 2.

So cyclic subgroups can have either finite or infinite order.

1.2 *Subgroup generated by a subset*

Lecture 2
August 17th, 2017
Notes by Sergio E. Garcia Tapia

Notation:

$$\langle A \rangle = \bigcap_{\substack{H' \leq G \\ H' \supset A}} H'.$$

1.15 proposition. *For $A \subseteq G$, let*

$$H = \{a_1 a_2 \cdots a_r | a_i \in A \text{ and } a_i^{-1}\} \cup \{e_G\} = H \cup \{e\}.$$

Then $\langle A \rangle = H$.

Proof. (1) $\langle A \rangle$ is a group and $A \subset \langle A \rangle$, from last lecture. By closure, all expressions of the form $a_1 a_2 \cdots a_r$ lie in $\langle A \rangle$, where $a_i \in A$ or $a_i^{-1} \in A$. From this, we obtain $H \subseteq \langle A \rangle$. Also, one can check explicitly that H is a subgroup. (In particular, if $a_1 a_2 \cdots a_r \in H$, then its inverse is $a_r^{-1} \cdots a_2^{-1} a_1^{-1}$, and it is contained in H as well). So in fact, $H \leq \langle A \rangle$.

(2) By part (1), H is a subgroup of G that contains A as a subset. Since $\langle A \rangle$ is the smallest subgroup of G satisfying this condition, $\langle A \rangle \leq H$.
Putting (1) and (2) together, we get $\langle A \rangle = H$. □

If for some $A \subset G$ we have $\langle A \rangle = G$, then we say that A generates G. In particular,

- If $|A| = 1$, then $\langle A \rangle$ is called a cyclic subgroup.
- If $|A| = 1$ and A generates G, then G is a cyclic group.

1.16 EXAMPLES. The sets $(\mathbb{Z}, +, 0) = \langle 1 \rangle$ and $(\mathbb{Z}/n\mathbb{Z}, +, 0) = \langle 1 \rangle$.

1.17 THEOREM. *If G is cyclic, then it is isomorphic to exactly one of the groups $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$. In particular,*

$$\mathbb{Z}/m\mathbb{Z} \ncong \mathbb{Z}/n\mathbb{Z}$$

if $m \neq n$.

Proof. Write $G = \langle \{a\} \rangle$. Define a homomorphism

$$\phi : \mathbb{Z} \to G \quad \text{by} \quad \phi(1) = a, \quad \phi(n) = a^n.$$

Check yourself that ϕ is a homomorphism. We proceed to check surjectivity and injectivity.

(1) ϕ is surjective: Since $G = \{a^i : i \in \mathbb{Z}\}$ and $a_i = \phi(i)$.

(Case 1) : ϕ is injective. This means that $\phi : \mathbb{Z} \to G$ is an isomorphism and therefore $G \cong \mathbb{Z}$.

(Case 2) : ϕ is not injective, so there exist $n, m \in \mathbb{Z}$ such that $m \neq n$ and

$$\phi(n) = \phi(m) \quad \Longrightarrow \quad a^m = a^n \quad \Longrightarrow \quad a^{m-n} = e_G = a^{n-m}.$$

Let k be the smallest positive integers such that $a^k = e_G$. Define $\overline{\phi} : \mathbb{Z}/k\mathbb{Z} \to G$ by

$$\overline{\phi}(\overline{m}) = a^m \quad \Longrightarrow \quad \overline{\phi}(\overline{m+k}) = a^{m+k} = a^m,$$

where $\overline{m}$ is the equivalence class of m with respect to mod k equivalence on $\mathbb{Z}$. Checking that $\overline{\phi}$ is a well-defined homomorphism is left as an exercise. It is also claimed that $\overline{\phi}$ is an isomorphism.

(1) $\overline{\phi}$ is surjective: Take any element $a^i \in G$, and set

$$i = nk + r, \quad 0 \leq r < k,$$

using the Euclidean division algorithm. Then

$$a^i = a^{nk+r} = a^r = \overline{\phi}(\overline{r}),$$

where $\overline{r}$ is again the equivalence class of r with respect to mod k equivalence.

(2) $\overline{\phi}$ is injective: Suppose that $\overline{\phi}(\overline{m}) = \overline{\phi}(\overline{m})$ (and without loss of generality that $m \geq n$). Then

$$a^m = a^n \quad \Longrightarrow \quad a^{m-n} = e_G.$$

Using the Euclidean division algorithm again to set $m - n = qk + r$, where $0 \leq r < k$, we have

$$a^{m-n} = a^{qk+r} = a^r = e_G.$$

But k is the positive integer such that $a^k = 1$, so we must have $r = 0$. Therefore,

$$m - n = qk \quad \Longrightarrow \quad \overline{m} = \overline{n},$$

thereby proving that $\overline{\phi}$ is injective, so $\overline{\phi} : \mathbb{Z}/k\mathbb{Z} \to G$ is an isomorphism, and we set $n = k$ to match the statement of our theorem.

□

remark. The integer k is the smallest positive power of a such that $a^k = e_G$, so $k = \text{order } (a)$.

1.18 definition. The *exponent* of a finite group G, $\exp(G)$, is the smallest $n \in \mathbb{N}$ such that $x^n = e_G$ for all $x \in G$. This exists since

$$\prod_{a \in G} ord(a)$$

is a finite upper bound since G is finite.

1.19 proposition. *(1) Let G be a finite Abelian group. Then G is cyclic if and only if $exp(G) = |G|$.*

(2) Any subgroup of a cyclic group is cyclic.

(3) If G is a cyclic group of order r and $H \leq G$, then $|H| \Big| r$, and for any $q|r$, there is exactly one subgroup of G of order q.
(Hint: Consider the smallest power of a that lies in H).

1.3 *Permutation groups*

Every permutation has a cycle decomposition into disjoint cycles. But, for example, $(13) = (12)(23)(12)$ is a valid cycle product. Also note that since $(123) = (312)$, we have $(123)(45) = (312)(45)$, but neither of this equals $(321)(45)$, since (321) is a distinct permutation than $(123) = (312)$.

1.20 definition. : 2-cycles (which are cycles of length 2) are also called *transpositions*.

1.21 THEOREM. *Any $g \in S_n$ can be expressed as a product of transpositions.*

Proof. By direct computation, one can verify that

$$(i_1 \cdots i_k) = (i_1 i_k)(i_1 i_{k-1}) \cdots (i_1 i_3)(i_1 i_2).$$

It is remarked that this product is not unique. □

1.22 DEFINITION. The sign of a permutation $g = t_1 \cdots t_k$, where each t_i is a transposition, equals

$$sgn(g) = \begin{cases} 1 & \text{if } k \text{ is even} \\ -1 & \text{if } k \text{ is odd.} \end{cases}$$

Actually, although this is presented as a definition, it should be proved. But before that, consider the homomorphism $\psi : S_n \to GL_n(\mathbb{R})$ defined by

$$\begin{pmatrix} 1 \to i_1 \\ 2 \to i_2 \\ \vdots \\ n \to i_n \end{pmatrix} \to \begin{matrix} \\ (\text{row } i_2) \\ \\ (\text{row } i_1) \end{matrix} \begin{pmatrix} 0 & 0 & \cdots \\ 0 & 1 & \cdots \\ \vdots & \vdots & \vdots \\ 1 & 0 & \cdots \\ 0 & 0 & \cdots \end{pmatrix}.$$

That is, the homomorphism puts 1 in the (i_k, k) spot. The map ϕ is invertible because it has one 1 in any row/column, so the columns are independent. For example, in S_3 we have

$$(123) \xrightarrow{\psi} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad (13) \xrightarrow{\psi} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Also, remark that

$$\phi(g) \cdot e_\ell = e_{g(\ell)}.$$

That is, multiplying the permuted matrix $\phi(g)$ by the basis vector e_ℓ yields the basis vector $e_{g(\ell)}$. As an example to see that ψ is operation-preserving, note that $(123)(12) = (23)$ and

$$\psi((123))\psi((13)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \psi((23)).$$

The homomorphism $\psi : S_n \to GL_n(\mathbb{R})$ is, in fact, injective. With ψ in mind, we note that $GL_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^*$ is a group homomorphism. Therefore we can define

the composite homomorphism

$$(\det \circ \psi) : S_n \xrightarrow{\psi} GL_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^* \iff (\det \circ \psi) : S_n \to \mathbb{R}^*.$$

One can show that this is well-defined. Furthermore, it satisfies

$$\text{identity permutation: } (1) \xrightarrow{\psi} I_n \xrightarrow{\det} 1,$$

$$\text{transposition: } (ab) \xrightarrow{\psi} \text{permuted } I_n \xrightarrow{\det} -1.$$

1.23 definition. If $g \in S_n$, then $sgn(g) = (\det \circ \psi)(g)$.

Using the operation-preserving property of these homomorphisms, we obtain for $g = t_1 \cdots t_k$

$$\begin{aligned}(\det \circ \psi)(t_1 \cdots t_k) &= \det(\psi(t_1)) \cdots \det(\psi(t_k)) \\ &= \prod_{i=1}^{k} (-1) \\ &= (-1)^k\end{aligned}$$

which agrees with the previous definition of $sgn(g)$.

Think of $(\det \circ \psi)$ as a map

$$S_n \to \{-1, 1\} \cong \mathbb{Z}/2\mathbb{Z},$$

where $\{-1, 1\}$ is considered a group under multiplication. The point of this is to define the *alternating group of degree n* denoted by A_n and given by

$$A_n \{g \in S_n | sgn(g) = 1\}.$$

Check that A_n is a subgroup of S_n.

1.24 exercise. $|A_n| = \frac{n!}{2}$.

In fact, A_n is the kernel of the homomorphism $(\det \circ \psi)$, where the kernel is the pre-image of the identity element.

1.4 *Group actions on sets*

Instead of the notation $G(S)$ for the set of bijective maps from S onto itself, we denote

$$\text{Sym } S := \{f : S \to S | f \text{ is bijective}\}.$$

1.25 definition. An *action* of G on a set S is a homomorphism

$$\alpha : G \to \text{Sym } S.$$

remark. Not necessarily injective. (If injective, α is called a *faithful* action).

1.26 examples. Let $s \in S$. Then

(1)

$$\begin{aligned}(\alpha(gh))(s) &= (\alpha(g)\alpha(h))(s)\\ &= \alpha(g)[\alpha(h)(s)].\end{aligned}$$

(2) $\alpha(e)(s) = s$.

Lecture 3
August 22nd, 2017
Notes by Joseph Dorta

Recall: If G is a group and S is a set, then a *G-action on S* is a homomorphism, $\alpha : G \to Sym(S)$.
In particular α has the following two properties:

(1) $\alpha(e) = id$

(2) $\alpha(gh) = \alpha(g) \cdot \alpha(h)$.

Similarly α gives rise to the map $\phi : G \times S \to S$ where $\phi(g, s) := \alpha(g)(s)$ satisfying:

(1*) $\phi(e, s) = s$

(2*) $\phi(gh, s) = \alpha(gh)(s) = \alpha(g)[\alpha(h)(s)] = \phi(g, \phi(h, s))$

Conversely, given a $\phi : G \times S \to S$ satisfying (1*) and (2*), we get an $\alpha : G \to Sym(S)$ satisfying (1) and (2).

Proof. Given a ϕ, we want$\alpha : G \to S$. For every $g \in G$ we want $\alpha(g) \in Sym(S)$.
Define $\alpha(g) : S \to \phi(g, s)$.
Let's check that α is a permutation/bijection which satisfies (1) and (2).

1. $\alpha(e) : s \mapsto \phi(e, s) = s$ by (1*), so that $\alpha(e) = id$, hence (1) is satisfied.
2. Let's check that (2) is satisfied, $\alpha(g) \circ \alpha(h)(s) = \alpha(g) \circ \phi(h, s) = \phi(g, \phi(h, s))$ by the definition of α. Further, $\phi(g, \phi(h, s)) = \phi(gh, s) = \alpha(gh)(s)$. This verifies property (2).
3. Now it is easy to check that $\alpha(g)$ is a bijection by admitting it's inverse. $\alpha(g) \circ \alpha(g^{-1}) = \alpha(gg^{-1})$ by (2) and $\alpha(gg^{-1}) = \alpha(e) = id$ by (1). Similarly $\alpha(g^{-1}) \circ \alpha(g) = id$.

□

Thus, we see that there are two ways to conceive of G-action on S as either a homomorphism $\alpha : G \to S$ or $\phi : G \times S \to S$. **Notation:** Suppose we have an action $\phi(g, s)$ denoted by $g \cdot s$, or simply gs.Then, we have (1*) $e \cdot s = s$ and (2*) $gh \cdot s = g \cdot (h \cdot s)$.

1.27 examples. (1) $G = gl_n(\mathbb{R})$ acts on $\mathbb{R}^n$ by letting $A \in gl_n(\mathbb{R})$ and $\vec{v} \in \mathbb{R}^n$ and allowing A to act on $\vec{v}$ by matrix multiplication called the standard action of $gl_n(\mathbb{R})$ on $\mathbb{R}^n$.

$$A \cdot \vec{v} = A\vec{v}$$

(2) $G = S^1 = \{$complex numbers of norm 1 $\}$or $\{\begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix}\}$.
Here $G \subset gl_2(\mathbb{R})$ so that S^1 acts on $\mathbb{R}^2$.

More generally, given an action of G on S and $H \leq G$, we get an action of H on S.

(3) Sym(S) *naturally* acts on S.

(4) Take $S = G$, G acts on S by left multiplication $\cdot : G \times S \to S$, explicitly $(g, s) \mapsto gs$.

So if $H \leq G$, then H also acts on G by left multiplication. Take $g \in G$ and consider the set $H_g := \{h \cdot g | h \in H\}$, called the *right H-coset of g* in G.

1.28 examples. $G = \mathbb{C}*$,$H = S^1$, then $S^1 \cdot g =$ the circle around 0with radius $|g|$.

Observations:

(1) $H \cdot e = H$

(2) Suppose $x \in Hy$, then $y \in Hx$. Since $x \in Hy \Rightarrow x = hy$ for some $h \in H$, then $y = h^{-1}x$
If $x \in Hy$ and $y \in Hz$,then $x \in Hz$.
Since $x \in Hy$ and $y \in Hz \Rightarrow x = hy$ and $y = h'z$ for some $h, h' \in H$, then $x = hh'z$.

Whence we see that being in the same coset is an equivalence relation on the elements of G. Thus the H-cosets partition G.// Now, suppose $g \in G$ and

$g' \in G$, we look at their cosets, Hg and Hg'. Then there is a bijection $Hg \leftrightarrow Hg'$ given by $x \mapsto xg^{-1}g'$ with inverse $y \mapsto yg'^{-1}g$.
So if G is finite, then the cosets have the same cardinality, namely $|H|$.

1.29 theorem. *(Lagrange's Theorem) Suppose G is a finite group and H is a subgroup of G. Then, $|G|$ =(number of H-cosets)$\times|H|$. In particular, $|H|$ divides $|G|$.*

Note that just as we defined right cosets, we can define left cosets.

1.30 definition. If G is a group, and $H \leq G$, then given $g \in G$, we say:

- $gH := \{gh|h \in H\}$ is called the **left coset** of H in G with respect to g.
- $Hg := \{hg|h \in H\}$ is called the **right coset** of H in G with respect to g.

1.31 definition. Let G act on a set S, then the set $G \cdot s := \{gs|g \in G\}$ is called the **orbit** of s under G.

Note that the orbit under left (resp. right) multiplication action is precisely a right (resp. left) coset. Further note that "being in the same orbit" is an equivalence relation, so orbits partition S. However, orbits need not have the same size. Returning to our example of S^1 acting on $\mathbb{C}$, we note that the orbit of the origin is itself, whereas the orbit of any other element is a circle centered at the origin with radius the norm of that element.
Examples:

(1) $G = gl_n((R)), S = \mathbb{R}^{n\times n} = M_{n\times n}((R))$
action 1: $\cdot : G \times S \to S$ given by $(A, B) \mapsto AB$
orbits:

- If $B = I_n$ then $G \cdot B = gl_n(\mathbb{R})$
- $G \cdot 0$ =$\{0\}$

action 2: Conjugation $(A, B) \mapsto ABA^{-1}$ gives an action of $gl_n(\mathbb{R})$ on $M_{n\times n}((R))$.
orbits:

- The orbit of I_n is again itself $\{I_n\}$
- $\begin{bmatrix}1 & 0\\ 0 & 2\end{bmatrix}$ has orbit $\{A \begin{bmatrix}1 & 0\\ 0 & 2\end{bmatrix} A^{-1}|A \in gl_n(\mathbb{R})\}$ =$\{$matrices with eigenvalues 1 and 2$\}$

1.32 exercise. Find all the remaining orbits of both actions.

1.33 definition. Let G be a group which acts on S, then the set $G_s := \{g \in G|g \cdot s = s\}$ is called the **stabilizer** of s in G.

Going back to our example of S^1 acting on $\mathbb{C}$ we have $G_x = \{e\}$ if x is not the origin and $G_{origin} = S^1$

Note that The stabilizer is always a subgroup of G.

1.5 *The Orbit-Stabilizer Theorem*

Lecture 4
August 24th, 2017
Notes by Komal Agrawal

Let G be a group, S be a set and let G act on S. We define $G \cdot s = \{g \cdot s | g \in G\}$ as the orbit of s and $G_s = \{g \in G | g \cdot s = s\}$ as the stabilizer of s. Now, let $g \cdot s = g' \cdot s = s'$. Then $g^{-1}g \cdot s = s$ and thus, $g^{-1}g \in G_s$. That is, $g' = gh$ for some $h \in G_s$. Conversely, if $g' = gh$, where $h \in G_s$, then $g \cdot s = g' \cdot s$.

1.34 conclusion. Two elements g, g' lie in the same left coset of $G_s \iff g \cdot s = g' \cdot s$. Hence, we get a bijection between the left cosets of G_s in G and the orbit of s

$$gG_s \mapsto hs$$

and

$$gG_s \leftarrow\!\shortmid s'$$

where $s' = g \cdot s$.

If G is finite and orbit is finite, then $|G| = |G \cdot s| \times |G_s|$. This is the orbit stabilizer theorem (OST).

1.35 remark. For the infinite version of the orbit stabilizer theorem we consider the topological structure of the group and conclude that $dim(G) = dim(G \cdot s) + dim(G_s)$.

1.36 example. Let G be the group of orientation preserving symmetries of a cube. Then we can find the $|G|$ by the above theorem. Let V be the set of vertices of the cube. Let G act on V. We know that the orbit of V is the entire set V, that is, $|G.v| = 8$ and the stabilizers of v are the three rotations about v by $120°, 240°, 360°$. Using the OST,

$$|G| = 8 \times 3 = 24.$$

Similarly, if we let F be the set of all faces of the cube and let G act on F, we get the same order of G.

1.37 exercise. Show that G is isomorphic to S_4.

1.6 *Free Groups*

Let S be a set. Then the "free group on S" denoted by F_S is defined as the collection (upto equivalence) of all finite expressions of the form $s_1^{\pm 1} s_2^{\pm 1} \dots s_n^{\pm 1}$ where each $s_i \in S$.

1.38 OBSERVATIONS.

(1) Equivalence is generated by striking adjacent ss^{-1} or $s^{-1}s$.

(2) It includes the "empty" expression $\emptyset$.

(3) Clearly, $S \subset F_s$.

The product rule of this group is concatenation. Inverses are generated as $(s_1 s_2 \dots s_n)^{-1} = (s_n^{-1} s_{n-1}^{-1} \dots s_1^{-1})$. F_s is clearly a group under these laws.

1.39 REMARK. F_S is not commutative as $ab \neq ba$ by definition.

1.40 EXAMPLE.

(1) $S = \{\emptyset\} \Rightarrow F_S = \{1\}$

(2) $S = \{a\} \Rightarrow F_S = \mathbb{Z}$

(3) $S = \{a, b\} \Rightarrow F_S = \mathbb{Z} * \mathbb{Z} \neq \mathbb{Z} \times \mathbb{Z}$

Let S be a set, then it's free group F_S has the following "universal property ": Given any group G and a function $\phi : S \to G$, there is a unique group homomorphism

$$\widetilde{\phi} : F_S \to G$$

which extends ϕ.

Proof. Let the word $s_1^{\pm 1} s_2^{\pm 1} \dots s_n^{\pm 1} \mapsto \phi(s_1^{\pm 1}) \phi(s_2^{\pm 1}) \dots \phi(s_n^{\pm 1})$ defines the $\widetilde{\phi} : F_S \to G$ homomorphism. □

1.41 EXAMPLE. Consider $S_3 = \{id, (12), (13), \dots\}$ Let $\phi : F_{ab} \to S_3$ such that $a \mapsto (12)$ and $b \mapsto (23)$. Then we say that (12) and (23) generate S_3 and ϕ is surjective.

1.7 *Kernels and Normal subgroups*

1.42 DEFINITION. The kernel K of a function is the preimage of the identity element of the codomain; that is, the subset of the domain consisting of all those elements of it that are mapped by the function to the identity element.

In the above example, we see that $a^2, b^2, (ab)^3 \in K$. If $a^2 \in K$, then $ba^2b^{-1} \in K$ and similarly, so does $(word)a^2(word)^{-1} \in K$. More generally, if $\phi : G \to H$ is

a homomorphism and $K = \ker\phi$, then for all $g \in G$ and $k \in K$, $gkg^{-1} \in K$, that is, $gKg^{-1} \subset K$ for all $g \in G$.

1.43 definition. We say a subgroup $K \leq G$ is normal if for all $g \in G$, $gKg^{-1} \subset K$.

1.44 example.

(1) $A_n \triangleleft S_n$ is normal as A_n is the kernel of the homomorphism $\phi : S_n \to \{1, -1\}$.

(2) The set $\{id, (12)(34), (13)(24), (14)(23)\} \triangleleft S_4$. It arises as the kernel of the homomorphism $\phi : S_4 \to S_3$ defined as follows: Consider the unordered $2+2$ partitions of $\{1,2,3,4\}$, that is, $\{\{1,2\},\{3,4\}\}$, $\{\{1,3\},\{2,4\}\}$ and $\{\{1,4\},\{3,2\}\}$. S_4 acts on this set and we get our desired homomorphism.

1.45 observation. If $K \triangleleft G$, then $gK = Kg$ as $gK = (gKg^{-1})g$.

1.8 *Quotient Groups*

Denote by $[g] = gK = Kg$. Then, $G/K = \{[g] | g \in G\}$. We can find a natural map $\phi : G \to G/K$ as $g \mapsto [g]$. In the above set, let $[g_1] = [g_1']$ and $[g_2] = [g_2']$, that is, $g_1' = k_1 g_1$ for some $k_1 \in K$ and $g_2' = k_2 g_2$ for some $k_2 \in K$. Multiplication can be defined as $[g_1] \cdot [g_2] = [g_1 \cdot g_2]$. We see that $[g_1'] \cdot [g_2'] = [g_1' \cdot g_2'] = [g_1 \cdot g_2]$. As $g_1' \cdot g_2' = k_1 g_1 k_2 g_2 = k_1 g_1 k_2 g_1^{-1} g_1 g_2 = k_1 k_3 g_1 g_2 = k_4 g_1 g_2$.

1.9 *The isomorphism theorems*

Lecture 5
August 29th, 2017
Notes by Jack Wagner

Let $H \triangleleft G$. Let us recall the construction of the quotient group G/H. Because H is a normal subgroup of G, we know that $gH = Hg$ for all $g \in G$. We will use the notation $[g]$ to denote the coset gH. Define a multiplication $G/H \times G/H \to G/H : ([g_1], [g_2]) \mapsto [g_1 g_2]$. We will show the following claims about this multiplication are true:

1. This is well defined.
2. This is associative and has and identity.
3. Inverses exist.

These claims show that G/H is a group under this multiplication.

Proof. 1. Suppose that $[g_1'] = [g_1]$ and $[g_2'] = [g_2]$. We want to show that $[g_1' g_2'] = [g_1 g_2]$. This gives us that $g_1' = g_1 h_1$, and $g_2' = g_2 h_2$ for some $h_1, h_2 \in H$. We can now see that $g_1' g_2' = g_1 h_1 g_2 h_2 = g_1 g_2 h_1' h_2$ for some $h_1' \in H$, because $H \triangleleft G$. Thus $[g_1' g_2'] = [g_1 g_2]$.

□

1.46 exercise. Prove the second and third claims about the multiplication on G/H.

We now have that G/H is a group. It is called the quotient group of G by H.

Recall that kernels of group homomorphisms are normal subgroups. We can now state and prove a few theorems about homomorphisms.

1.47 theorem. *(First isomorphism theorem) Let $\phi : G \to H$ be a surjective group homomorphism, and let $\ker(\phi) = K$, then $G/K \cong H$.*

Proof. Let $\phi : G \to H$ be a surjective homomorphism with kernel K. Define $\bar{\phi} : G/K \to H : [g] \mapsto \phi(g)$. We need to show that, (1) $\bar{\phi}$ is a well-defined homomorphism, (2) it is injective, and (3) it is surjective.

(1) Suppose $[g'] = [g]$. This means $g' = gk$ for some $k \in K$, so we get that

$$\bar{\phi}([g']) = \phi(g') = \phi(gk) = \phi(g)\phi(k) = \phi(g) = \bar{\phi}([g]).$$

Thus the function is well defined. It is clear that it is a homomorphism because ϕ is a homomorphism.

(2) Let $[g] \in G/K$ such that $\bar{\phi}([g]) = 1$. Then $\phi(g) = 1$, so $g \in K$, and $[g] = [1]$. This shows that $\bar{\phi}$ is injective.

(3) Recall that ϕ is surjective, so for any $h \in H$, we know that $\phi(g) = h$ for some $g \in G$. Thus $\bar{\phi}([g]) = \phi(g) = h$, so $\bar{\phi}$ is surjective.

These three facts give us that $\bar{\phi}$ is an isomorphism, and therefore $G/K \cong H$. □

1.48 theorem. *(Universal property of quotient groups) Let $H \lhd G$. Suppose that G' is another group, and there is a group homomorphism $\phi : G \to G'$ such that for any $h \in H$, we get $\phi(h) = 1$ (ie $H < \ker(\phi)$). Then, there is a unique group homomorphism $\bar{\phi} : G/H \to G'$ such that the following diagram commutes:*

$$\begin{array}{ccc} G & \xrightarrow{\phi} & G' \\ \downarrow{\scriptstyle q} & \nearrow_{\bar{\phi}} & \\ G/H & & \end{array}$$

In other words, $\bar{\phi} \circ q = \phi$, where $q : G \to G/H : g \mapsto [g]$.

1.49 remark. Another way to say this is that if $H < \ker(\phi)$, the ϕ factors through G/H. Note that there are a lot of homomorphisms between G/H and G'. The uniqueness of $\bar{\phi}$ depends on (1) $\phi : G \to G'$, and (2) $H < \ker(\phi)$.

This theorem is important because if we are given a group that looks like a quotient, G/H, then we can create maps for G and use those to find maps for G/H. We will now outline the proof with some details left as an exercise.

Proof. Define $\bar{\phi}$ by $\bar{\phi}([g]) = \phi(g)$. Checking that it is a well defined group homomorphism is similar to the process used in the previous proof, and is left as an exercise.

(1) To see that $\bar{\phi} \circ q = \phi$, let $g \in G$. So $(\bar{\phi} \circ q)(g) = \bar{\phi}([g]) = \phi(g)$. Thus $\bar{\phi} \circ q = \phi$.

(2) To show uniqueness, let $\psi : G/H \to G'$ be some other map where $\psi \circ q = \phi$. If $g \in G$, then $\psi([g]) = (\psi \circ q)(g) = \phi(g) = \bar{\phi}([g])$. This is true for any g, so $\psi = \bar{\phi}$.

□

1.50 theorem. *(Second isomorphism theorem) Let $H \triangleleft G$ and $K < H$ such that $K \triangleleft G$. Consequently, $K \triangleleft H$. Then $G/H \cong (G/K)/(H/K)$.*

Proof. Let $\phi : G/K \to G/H$ where $\phi(gK) := gH$. We need to do the following:

(1) Show ϕ is a well defined homomorphism.

(2) Show $\ker(\phi) = H/K$.

(3) Show ϕ is surjective.

(4) Get $\bar{\phi} : (G/H)/(H/K) \to G/H$ uniquely, where $\bar{\phi}$ is an isomorphism using the previous theorems.

These details are left as an exercise. Once they are shown, the result is proven. □

1.51 theorem. *(Third isomorphism theorem) Let $H < G$ and $K \triangleleft G$, then*

(1) $HK = \{hk | h \in H, k \in K\}$ is a subgroup, and

(2) $HK/K \cong H/(H \cap K)$

1.52 exercise. Prove the third isomorphism theorem, and complete the proofs of the second isomorphism theorem and the universal property of quotient groups.

1.10 *Presentation of a Group by Generators and Relations*

Let G be a group, and let S be a set of generators of G, so $G = \langle S \rangle$. Let F_S be the free group on S. There exists a surjective group homomorphism $\phi : F_s \to G$ where $\phi(s) = s$. Now let $K_S = \ker(\phi)$. We know from the first isomorphism

theorem that $G \cong F_S/K_S$. This is called the presentation of G by generators and relations.

1.53 example. We can show that $S_3 = \langle (12), (23) \rangle$. Let $a = (12)$ and $b = (23)$. The generating set of S_3 then is $\{a, b\}$, and the set of relations is $\{a^2, b^2, ababab\}$. We can present S_3 as the following: $S_3 = \langle a, b | a^2, b^2, ababab \rangle$.

1.11 *Back to Group Actions*

Recall that the conjugation action of G on itself is a map $G \times G \to G$ where $(h, g) \mapsto hgh^{-1}$. Let $g \in G$. The conjugacy class of g is $C(g) = \{hgh^{-1} | h \in G\}$. In other words, it is the orbit of the conjugation action. One can show that the conjugacy classes partition G. Let S be a set of representatives of the conjugacy class. This gives us that

$$G = \coprod_{g \in S} C(g).$$

1.54 example. The conjugacy classes of S_3 are $\{(1)\}$, $\{(12), (13), (23)\}$, and $\{(123), (132)\}$.

Recall that if $\sigma \in S_n$, then $\sigma(i_1 i_2 ... i_k)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)...\sigma(i_k))$. This helps prove the next theorem.

1.55 theorem. *The conjugacy classes of S_n are given by distinct cycle types.*

1.56 example. The representatives of the conjugacy class of S_4 are (1), (12), $(12)(34)$, (123), (1234).

1.57 theorem. *Let G be finite. Let S be a set of representatives of the conjugacy classes of G. Then*

$$|G| = \sum_{g \in S} |C(g)|.$$

This is called the class equation.

1.58 remark. By the orbit-stabilizer theorem, the size of the conjugacy class of x is $|G|/|Z_x(G)|$, and it thus divides $|G|$. This means that if S is a set of representatives of orbits for elements not in the center, then

$$|G| = |Z(G)| + \sum_{g \in S} |C(g)|$$

2 Sylow theory

Lecture 6
August 31st, 2017
Notes by Freddy Saia

Now that we have discussed much of the basics of group theory, including basic definitions, homomorphisms, isomorphism theorems, and quotient groups, we

turn to a more difficult task: the classification of all finite groups. The ultimate goal here is to determine all of the isomorphism classes of groups of any given finite order. This goal is certainly out of reach for this course, but that does not mean there is not some progress to be made. For example:

(i) We have already classified all cyclic groups, and have shown that all groups of prime order are cyclic.

(ii) We will later classify all finite abelian groups via the Fundamental Theorem of Finite Abelian Groups, which will turn out to be a specific case of a fundamental theorem in module theory.

Our main tool for further chipping away at the classification question will be the Sylow Theorems. We will provide and prove these theorems in this section, but first we give some motivation.

Lagrange's Theorem tells us that the order of a subgroup of any finite group divides the order of the group. One natural question is whether the converse of this statement holds: if $|G| = m$ and $n \mid m$, does G have a subgroup of order n? The answer in general is no. For example, the complete subgroup lattice of A_4 shown in 2 shows that A_4 has no subgroup of order 6, despite the fact that $6 \mid 12 = |A_4|$.

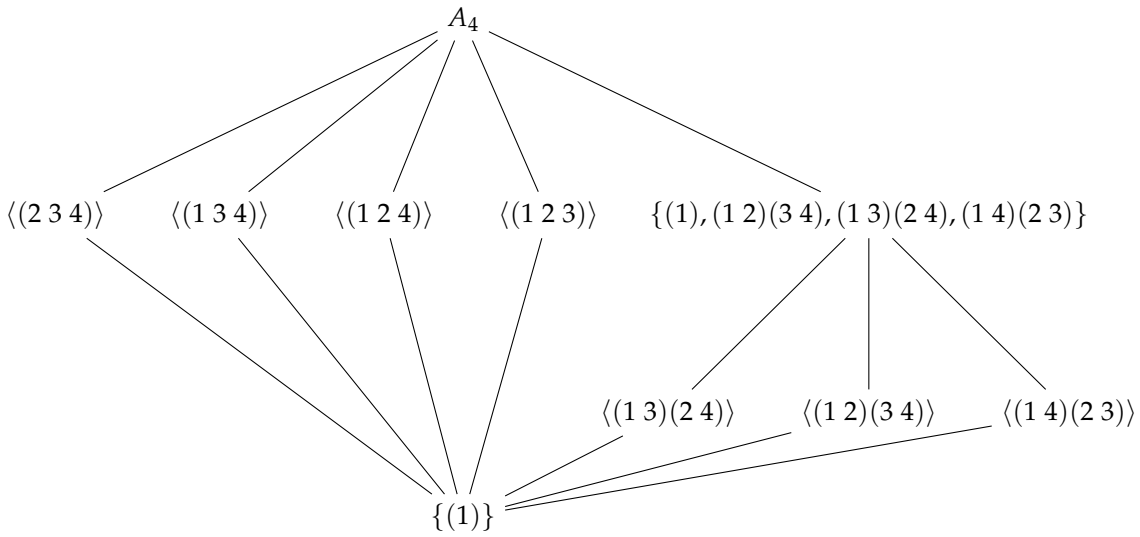


Figure 1: Subgroups of A_4

There are partial converses to Lagrange's Theorem, though, and this is precisely where the Sylow Theorems come in. We now give their statements:

2.1 theorem (Sylow theorems). *Let G be a finite group, then the following hold:*

(1) If p is a prime and $p^k \mid |G|$ for some $k \geq 0$, then G has a subgroup of order p^k. If k is the maximal power of p dividing $|G|$, we will call any subgroup of G of order p^k a Sylow p-subgroup of G.

(2) If $H_1, H_2 \leq G$ are two Sylow p-subgroups of G, then H_1 and H_2 are conjugate, i.e. there is a $g \in G$ such that $gH_1g^{-1} = H_2$. Note that this implies that if a group has a unique Sylow p-subgroup, then that subgroup is normal.

(3) If $|G| = p^k m$, where $p \nmid m$, and if n is the number of Sylow p-subgroups of G, then $n \mid m$ and $n \equiv 1 \pmod{p}$.

Before proving these theorems, we will tackle two propositions and one lemma as "warm-ups," with the latter being useful for the theorems' proofs.

2.2 PROPOSITION. *If p, q are primes and $|G| = pq$ with G non-abelian, then $Z(G) = \{e\}$.*

Proof. By Lagrange's Theorem, we know that $|Z(G)| \in \{1, p, q, pq\}$. We want to prove that $|Z(G)| = 1$, so we show that the other cases are not possible:

1. If $|Z(G)| = pq$, then G is abelian, contradicting our assumption.

2. If $|Z(G)| = p$, then

$$|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{pq}{p} = q.$$

   This means that $G/Z(G)$ is cyclic, though, which implies that G is abelian, again yielding a contradiction.

3. If $|Z(G)| = q$ then we get that the quotient $G/Z(G)$ is cyclic of order p just as in case (ii), and reach the same type of contradiction.

□

2.3 PROPOSITION. *If $|G| = p^k$ for p a prime and $k > 0$, then $Z(G) \neq \{e\}$.*

Proof. Suppose $Z(G) = \{e\}$, then the class equation says

$$|G| = |Z(G)| + \sum_{\substack{\text{conj class} \\ \text{reps } g \neq e}} [G : Z_g(G)].$$

Each term in the sum must be some non-trivial power of p by Lagrange's

Theorem, so we find

$$\begin{aligned} p^k &= 1 + \sum_{i=1}^{k-1} c_i p^i \\ &= 1 + p \sum_{i=1}^{k-1} c_i p^{i-1}. \end{aligned}$$

This implies that $p \mid 1$, which is a contradiction as p is prime. □

2.4 Lemma. *If G is abelian and $p \mid |G|$, then G has a subgroup of order p.*

Proof. We begin by noting that this is equivalent to showing that G has an element of order p, as any group of prime order is cyclic.

Suppose there is some $a \in G$ such that $\text{ord}(a) = pm$ for some m. This would mean that a^m has order p in G, as

$$(a^m)^p = a^{mp} = e$$

and mp is the lowest power of a giving the identity.

Using this fact, we will prove our lemma by downward induction on the order of our group. The base case of our induction is when $|G| = p$, in which case the lemma clearly holds.

Suppose that the result holds for all groups of order less than that of G. If we then have a nontrivial element $a \in G$ such that $p \nmid \text{ord}(a)$, then since G is abelian we may consider the quotient $G/\langle a \rangle$. Since $p \mid |G|$ but $p \nmid \langle a \rangle$, as $|\langle a \rangle| = \text{ord}(a)$, it follows that $p \mid |G/\langle a \rangle|$. Because $a \neq e$, this quotient is smaller than G, allowing us to apply our induction hypothesis. From this we get an element $b \in G$ such that $\pi(b)$ has order p in the quotient, where

$$\pi : G \to G/\langle a \rangle$$

is the standard quotient map. If $\text{ord}(b) = r$ in G, then

$$\pi(b)^r = \pi(b^r) = \pi(e)$$

implying $p \mid r$. Hence, $\text{ord}(b) = r = pm$ for some m. From here we apply the initial fact we proved above, finding that b^m has order p in G and completing our induction proof. □

We now move on to proofs of the individual Sylow Theorems, separated by examples of their applications.

Proof of Sylow Theorem (1). We let G be a given finite group and p a prime such that $p^k \mid |G|$ for some $k \geq 0$. Similar to the proof of the lemma above, we will prove this theorem by downward induction on $|G|$. The base cases of $k = 0, 1$

are relatively simple, as for $k = 0$ the trivial subgroup is a subgroup of order p^k and for $k = 1$ the lemma we just proved applies.

Assuming that the result holds for all groups of order less than that of G, we assume $k > 1$ and proceed into two cases.

(i) In our first case we suppose that $p \mid |Z(G)|$. Since $Z(G)$ is abelian, it follows from our lemma that $Z(G)$ has a subgroup K of order p. Since H is contained in the center it is abelian, and therefore it is normal in G. We then set $G' = G/K$, noting that G' has order $|G|/p$. This means that $p^{k-1} \mid |G'|$. Because $|G'| < |G|$, our induction hypothesis then provides us with a subgroup H' of G' of order p^{k-1}. With $\pi : G \to G'$ the quotient map, we let

$$H = \pi^{-1}(H') = \{h \in G \mid \pi(h) \in H'\}.$$

Note that H is a subgroup of G, that $K \leq H$, and that $H' \cong H/K$ by the first isomorphism theorem as $K = \ker(\pi|_H)$. This means that

$$|H| = |H'||K| = p^{k-1}p = p^k$$

giving us the subgroup we needed.

(ii) The other case is when $p \nmid |Z(G)|$. From the class equation

$$G = Z(G) + \sum_{\substack{\text{conj class} \\ \text{reps } g \notin Z(G)}} [G : Z_g(G)]$$

we see that this means there must be some $g \in G$ with $g \notin Z(G)$ such that

$$p \nmid [G : Z_g(G)] = \frac{|G|}{|Z_g(G)|}.$$

Because $p^k \mid |G|$, it follows that $p^k \mid |Z_g(G)|$. As $g \notin Z(G)$, we know $Z_g(G) \neq G$, so by induction there is some $H \leq Z_g(G)$ with $|H| = p^k$. Since $H \leq G$, the proof is complete.

□

2.5 EXAMPLE. The group S_4 has order $24 = 2^3 \cdot 3$. The first Sylow Theorem hence guarantees that S_4 has subgroups of orders $2, 3, 4$, and 8. Indeed, we have:

ORDER 2: $\langle (1\ 2) \rangle$

ORDER 3: $\langle (1\ 2\ 3) \rangle$

Order 4: $\langle (1\ 2\ 3\ 4) \rangle$

Order 8: The dihedral group D_8 of order 8, i.e. the group of symmetries of the square, embeds into S_4 as

$$D_8 \cong \langle (1\ 2\ 3\ 4), (1\ 2)(3\ 4) \rangle$$

with $(1\ 2\ 3\ 4)$ corresponding to a rotation by 90° and $(1\ 2)(3\ 4)$ corresponding to a reflection about the vertical axis if we number our vertices clockwise starting at the upper-left vertex.

Lecture 7
September 5th, 2017
Notes by Nolan Schock

We now turn to the task of proving Sylow's second and third theorems. Before the proof, we need to introduce the concept of a normalizer.

2.6 definition. If $P < G$, then the *normalizer* of P in G, denoted $N_G(P)$, is the set

$$N_G(P) = \{g \in G \mid gPg^{-1} = P\}.$$

The normalizer is the largest subgroup of G in which P is normal. Remark the following easy observations.

2.7 observations.

- $N_G(P) < G$
- $P < N_G(P)$
- $P \triangleleft N_G(P)$
- $P \triangleleft G \iff N_G(P) = G$

2.8 Lemma. *Let $P \in \mathbb{S}_p$. Suppose $H < N_G(P)$ is such that $|H| = p^\ell$ for some $\ell \in \mathbb{Z}^+$. Then $H < P$.*

Proof. Consider the set $HP = \{hp \mid h \in H, p \in P\}$. Then $HP < N_G(P)$ because $P \triangleleft N_G(P)$. We claim that $HP/P \cong H/(H \cap P) \cong \{e\}$.

To see this, note that $|H| = p^\ell$, $|P| = p^k$, and $|H \cap P| = p^a$ for some $a \in \mathbb{Z}_{\geq 0}$. Then $|HP| = p^\ell p^k p^{-a} = p^{k+\ell-a}$. Since $H \cap P \subseteq H$, we know that $l \geq a$. But if $l > a$, then $|HP| = p^{k+\ell-a} > p^k$, contradicting that P is a Sylow p-subgroup.

Therefore, $\ell = a$, so $H/(H \cap P)$ is trivial. We conclude that $H \cap P = H$, hence $H < P$. □

At last, we come to the proofs of Sylow's second and third theorems. The proof strategy will rely on considering the action of G on $\mathbb{S}_p$ by conjugation: If $g \in G$ and $H \in \mathbb{S}_p$, then the action $G \times \mathbb{S}_p \to \mathbb{S}_p$ is given by $(g, H) \mapsto gHg^{-1}$.

If $P \in \mathbb{S}_p$, we will also consider the conjugation action of P on $\mathbb{S}_p$ constructed by restricting the action of G. In detail, this action is given by the composition

$$P \times \mathbb{S}_p \longrightarrow G \times \mathbb{S}_p \longrightarrow \mathbb{S}_p,$$

where the first map $P \times \mathbb{S}_p \to G \times \mathbb{S}_p$ is the natural inclusion map in the first coordinate and the identity in the second, and the second map $G \times \mathbb{S}_p \to \mathbb{S}_p$ is the conjugation action of G on $\mathbb{S}_p$.

Proof of Sylow II,III. Fix $P \in \mathbb{S}_p$ and consider the action of P on $\mathbb{S}_p$ described above. For any $P' \in \mathbb{S}_p$, let $C(P')$ denote the orbit of P' under conjugation by P. (That is, $C(P') = \{gP'g^{-1} \mid g \in P\} < \mathbb{S}_p$.)

Note that $C(P) = \{P\}$ and, by the orbit-stabilizer theorem, $|C(P')|$ divides $|P| = p^k$ for any $P' \in \mathbb{S}_p$.

We first claim that if $P' \neq P$, then $|C(P')| > 1$. Suppose not, i.e. $C(P') = \{P'\}$. Then $gP'g^{-1} = P'$ for all $g \in P$, so $P < N_G(P')$. But then by the lemma $P < P'$. But P' and P are both Sylow p-subgroups, so they have the same order, which implies that $P = P'$, a contradiction. Therefore $|C(P')| > 1$ for all $P' \neq P$; since $|C(P')|$ divides p^k, we conclude that p divides $|C(P')|$.

Now, $\mathbb{S}_p$ is the disjoint union of the conjugacy classes of each $P' \in \mathbb{S}_p$. Combining the previous results, we thus see that

$$|\mathbb{S}_p| = n_p \equiv 1 \pmod{p},$$

proving the first part of Sylow III.

We now prove Sylow II. Look at the action of conjugation by G on $\mathbb{S}_p$, and let $C_G(P')$ denote the orbit under conjugation by G of P'. We want to show that $C_G(P) = \mathbb{S}_p$.

We again have that $\mathbb{S}_p = \coprod C_G(P')$, where each P' is the representative of a distinct conjugacy class. Suppose that there is a $P' \in \mathbb{S}_p \setminus C_G(P)$. Look at the action of P' on $C_G(P)$ (restricting the action of G on $\mathbb{S}_p$, and break up $C_G(P)$ into disjoint P'-orbits under this action, each having size p^{ℓ_i}, where $\ell_i > 0$ because of the previous argument. By summation, p divides $|C_G(P)|$. Now look at the action of P on $C_G(P)$. This time, the orbit of P has size 1, and the orbit of anything else has size p^{ℓ_i}, $\ell_i > 0$, by the same logic. Therefore, p divides $|C_G(P)|$ and $|C_G(P)| \equiv 1 \pmod{p}$, a contradiction. We conclude that $C_G(P) = \mathbb{S}_p$, proving Sylow II.

Finally, we prove the second part of Sylow III, that $n_p \mid m$. Let $P \in \mathbb{S}_p$. Then the orbit $C_G(P)$ of P under the conjugation action of G has size n_p. The stabilizer of P is $N_G(P)$, and $P < N_G(P)$. Thus the orbit-stabilizer theorem gives $n_p = \frac{|G|}{|N_G(P)|}$. Since $|G| = p^k m$ and $|N_G(P)| = p^k m'$ for some m', we conclude that $n_p = \frac{m}{m'} \in \mathbb{Z}$, i.e. $n_p \mid m$, as desired. □

2.9 EXAMPLE. The group A_4 has order $12 = 2^2 \cdot 3$. If n_2 is the number of Sylow

2-subgroups of A_4, then Sylow III states that $n_2 \mid 3$ and $n_2 \equiv 1 \pmod 2$, together implying that $n_2 = 1$ or 3. We previously saw, by inspection, that A_4 has precisely one subgroup of order 4, hence $n_2 = 1$.

On the other hand, the group D_{12} of symmetries of the hexagon has the same order, hence $n_2 = 1$ or 3 in this case as well. But here $n_2 = 3$, which can be seen by considering the three possible embedding of a square into the hexagon.

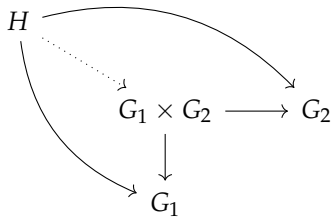
We conclude that $A_4 \ncong D_{12}$.

3 Direct and semidirect products

3.1 *Direct products*

If G_1, G_2 are groups, then the direct product group is the set $G_1 \times G_2$ with coordinate-wise multiplication $(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2)$.

The direct product is a universal object in the sense that, if H is a group with maps $H \to G_1$ and $H \to G_2$, then these maps "factor uniquely" through $G_1 \times G_2$. More precisely, the following diagram commutes, where $G_1 \times G_2 \to G_1$ is the natural projection map $(g_1, g_2) \mapsto g_1$, and similarly for $G_1 \times G_2 \to G_2$.



3.1 observations.

- $G_1 \cong G_1 \times \{e_{G_2}\} \lhd G_1 \times G_2$
- $G_2 \cong \{e_{G_1}\} \times G_2 \lhd G_1 \times G_2$
- $G_1 \cap G_2 = \{(e, e)\}$.

3.2 proposition. *Let G be a group and let $H, K \lhd G$ such that*

1. *$H \cap K = \{e\}$, and*
2. *$HK = G$.*

Then $G \cong H \times K$.

Proof. Define the map $\varphi : H \times K \to G$ by $\varphi(h, k) = hk$. Then φ is surjective because $HK = G$ and injective because $H \cap K = \{e\}$. We want to show that φ is a group homomorphism.

Suppose that $h \in H$ and $k \in K$. Notice that $h \in H$ and $kh^{-1}k^{-1} \in H$ because H is normal, so their product $hkh^{-1}k^{-1} \in H$. This is also equal to $(hkh^{-1})k^{-1}$, and $hkh^{-1}, k^{-1} \in K$ because K is normal. So $hkh^{-1}k^{-1} \in K$. Thus $hkh^{-1}k^{-1} \in H \cap K = \{e\}$, so $hkh^{-1}k^{-1} = e$, so $hk = kh$.

Now, let $(h_1, k_1), (h_2, k_2) \in H \times K$. Then

$$\begin{aligned}\varphi((h_1,k_1)(h_2,k_2)) &= \varphi(h_1h_2, k_1k_2)\\ &= h_1h_2k_1k_2\\ &= h_1k_1h_2k_2\\ &= \varphi(h_1,k_1)\varphi(h_2,k_2),\end{aligned}$$

so φ is a homomorphism. □

3.2 *Semidirect products*

Lecture 8
September 7th, 2017
Notes by Terrin Warren

We have discussed how to construct a group which is formed by two normal subgroups H, K of a given group G. Now we will examine a construction of a group G, that is formed from two subgroups H and K where only one of H or K is normal in G.

3.3 definition. If $H \triangleleft G, K < G$, and

1. $H \cap K = \{e\}$
2. $HK = G$,

then G is called the *inner semidirect product* denoted by $G = H \rtimes K$.

3.4 remark. Notice that if (h_1k_1) and (h_2k_2) are elements of $G = HK$, then their product is also in G.

$$(h_1k_1)(h_2k_2) = h_1k_1h_2(e)k_2 = h_1k_1h_2(k_1^{-1}k_1)k_2 = h_1(k_1h_2k_1^{-1})k_1k_2$$

Then since $H \triangleleft G$, we know that $k_1h_2k_1^{-1} \in H$ so $h_1(k_1h_2k_1^{-1}) \in H$ and $k_1k_2 \in K$, thus the product is in $G = HK$ as desired.

Now, more generally we want to construct the *outer semidirect product* $G = H \rtimes K$ of any two groups H and K. We begin with the function $K \times H \to H$ given by $(k, h) \mapsto (khk^{-1})$. We want this function to be a group action, which means we want a function from K to $\mathrm{Sym}(H)$.

3.5 definition. Given a group H, we define the set of automorphisms of H to be the set of all isomorphisms from H to H, denoted by $\mathrm{Aut}(H)$. This is a group whose operation is composition and identity element is the identity map.

We need to specify a homomorphism $\phi : K \to \mathrm{Aut}(H)$.

3.6 exercise. The homomorphism $K \times H \to H$ given by $(k, h) \mapsto (khk^{-1})$ is an automorphism on H.

3.7 example. Let $H = \mathbb{Z}/3\mathbb{Z} = \{1, a, a^2\}$. Then

$$\mathrm{Aut}(H) = \{f : H \to H | \text{ f is an isomorphism}\}$$

$$\mathrm{Aut}(H) = \left\{ \begin{pmatrix} 1 \to 1 \\ a \to a \\ a^2 \to a^2 \end{pmatrix}, \begin{pmatrix} 1 \to 1 \\ a \to a^2 \\ a^2 \to a \end{pmatrix} \right\} = \{id, \sigma\}$$

Notice that $\mathrm{Aut}(H)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and moreover it is a subgroup of $\mathrm{Sym}(\mathbb{Z}/3\mathbb{Z}) \cong \mathrm{S}_3$.

Suppose we have two groups H and K with a group homomorphism $\phi : K \to \mathrm{Aut}(H)$. Then we define the ϕ-semidirect product as follows.

3.8 definition. The *ϕ-semidirect product*, denoted by $H \rtimes_\phi K$, is defined to be the group with the following properties:

1. The set is $H \times K$.

   i.e. the elements are of the form $\{(h, k) | h \in H, k \in K\}$.

2. If $(h_1, k_1), (h_2, k_2) \in H \rtimes_\phi K$ then the operation is given by:
   $(h_1, k_1)(h_2, k_2) = (h_1 \phi_{k_1}(h_2), k_1 k_2)$.

3. The identity element is given by (e, e).

3.9 claim. *$H \rtimes_\phi K$ is a group.*

Proof. 1. Identity:

$$(e, e)(h, k) = (e\phi_e(h), ek) = (\phi_e(h), k) = (h, k)$$

where ϕ_e is the identity automorphism. For the other direction we have

$$(h, k)(e, e) = (h\phi_k(e), ke) = (h, k)$$

where for any $k \in K, \phi_k : H \to H$ is a group homomorphist so $\phi_k(e) = e$.

2. Associative: For the first choice of grouping we have

$$\begin{aligned}(h_1,k_1)[(h_2,k_2)(h_3,k_3)] &= (h_1,k_1)(h_2\phi_{k_2}(h_3,k_2k_3)\\ &= (h_1\phi_{k_1}(h_2\phi_{k_2}(h_3)),k_1k_2k_3)\\ &= (h_1\phi_{k_1}(h_2)\phi_{k_1}\circ\phi_{k_2}(h_3),k_1k_2k_3).\end{aligned}$$

For the second choice of grouping, we have

$$\begin{aligned}[(h_1,k_1)(h_2,k_2)](h_3,k_3) &= (h_1\phi_{k_1}(h_2,k_1k_2)(h_3,k_3)\\ &= (h_1\phi_{k_1}(h_2)\phi_{k_1k_2}(h_3),k_1k_2k_3)\\ &= (h_1\phi_{k_1}(h_2)\phi_{k_1}\circ\phi_{k_2}(h_3),k_1k_2k_3).\end{aligned}$$

We have equality, so the operation is associative as desired.

3. Inverses: We can find the inverse of the element (h,k) by finding (x,y) that satisfy the following expression:

$$(x,y)(h,k) = (e,e)$$

So we must have $(x\phi_y(h),yk) = (e,e)$. Since $yk = e_k$ we have $y = k^{-1}$.
Then replacing y with k^{-1} in the above equation gives $x\phi_{k^{-1}}(h) = e$, so we have
$x = (\phi_{k^{-1}}(h))^{-1} = \phi_{k^{-1}}(h^{-1})$.
The inverse of (h,k) is given by $(\phi_{k^{-1}}(h^{-1}),k^{-1})$.

□

3.10 EXERCISE. Verify that the product $(h,k)(\phi_{k^{-1}}(h^{-1}),k^{-1})$ is equal to the identity.

3.11 OBSERVATION. Now we can make some observations about the subgroups of the group $H \rtimes_\phi K$

1. $K < H \rtimes_\phi K$. We can see this by noticing that for any $k \in K$, $k \mapsto (e,k)$.
2. $H \triangleleft H \rtimes_\phi K$ We can see this by noticing that for any $h \in H$, $h \mapsto (h,e)$. Suppose $(a,b) \in H \rtimes_\phi K$. Then we have

$(a,b)(h,e)(\phi_{b^{-1}}(a^{-1}),b^{-1}) =$
$(a\phi_b(h),b)(\phi_{b^{-1}}(a^{-1}),b^{-1}) =$
$(a\phi_b(h)\phi_b(\phi_{b^{-1}}(a^{-1})),bb^{-1}) =$
$(a\phi_b(h)a^{-1},e).$

Then using the fact that $a \in H$ we conclude that $a\phi_b(h)a^{-1} \in H$. Thus, $(a\phi_b(h)a^{-1}, e) \in H \times \{e\}$ and $H \triangleleft H \rtimes_\phi K$.

3.12 exercise. Let $H \triangleleft G, K < G$, and suppose $H \cap K = e, HK = G$ and let $\phi : K \to \mathrm{Aut}(H)$ be the conjugation map such that $\phi_k(h) = khk^{-1}$. Then $G \cong H \rtimes_\phi K$. Give a group homomorphism from G to $H \rtimes_\phi K$ and show that it is an isomorphism.

3.3 *Exact Sequences*

3.13 definition. Let $\phi : A \to B$ be a group homomprphism and $\psi : B \to C$ be a group homomorphism. Then

$$A \xrightarrow{\phi} B \xrightarrow{\psi} C$$

is said to be *exact* at B if the following are true:

1. $\psi(\phi(a)) = \mathrm{id}_c$
2. $\ker \psi = \mathrm{im}\, \phi$.

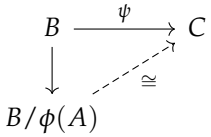
3.14 definition. We say that

$$1 \to A \xrightarrow{\phi} B \xrightarrow{\psi} C \to 1$$

which is exact at A, B, and C, is a *short exact sequence*

Using the fact that the chain is exact at B we have $\ker \phi = \mathrm{im}\, \phi$. The exactness at A implies that $\ker \phi = \{\mathrm{id}\}$, i.e. ϕ is injective. Similarly, the exactness at C implies that $\mathrm{im}\, \phi = C$, i.e. ψ is surjective.

Using the fact that ϕ is injective, we have $A \cong \phi(A)$, which means we can think of A as a subgroup of B since $\phi(A) < B$. This gives us the following:



using the funcamental isomorphism theorem or the universal property. Then we have $C \cong B/A$.

Now we can connect what we have done with direct and semidirect products to these exact sequences.

3.15 claim. *Let $G = H \times K$, then there exists a short exact sequence*

$$1 \to H \to G \to K \to 1.$$

such that for $h \in H$ and $(h, k) \in G$, we have $h \mapsto (h, e)$ and $(h, k) \mapsto k$.

Similarly to the example, we want $K = G/H$. Since $G = HK$, we have $G/H = HK/H$, then the fundamental isomorphism theorem implies that $HK/H = K/H \cap K$ where $H \cap K = \{e\}$ by assumption. Thus $G/H = K$ as desired.

3.16 CLAIM. *Let $G = H \times K$, then there exists another short exact sequence*

$$1 \to K \to G \to H \to 1.$$

Similarly for some semidirect product given by $G = H \rtimes_\phi K$ there is a short exact sequence given by

$$1 \to H \to G \to K \to 1.$$

In general, in N is a normal subgroup of G, then we have

$$1 \to N \to G \to G/N \to 1.$$

If N is known, then you can try to rebuild G from that information. However, knowing some exact sequence of groups does not necessarily imply that there is a direct of semidirect product formed from the groups.

3.4 *Split exact sequences and semidirect products*

Lecture 9
September 14th, 2017
Notes by Asilata Bapat

Recall that a semidirect product $G = H \rtimes_\alpha K$ yields a short exact sequence

$$1 \to H \to G \to K \to 1.$$

We now characterize all short exact sequences that arise from semidirect products.

3.17 DEFINITION. A *splitting* of a short exact sequence

$$1 \to H \xrightarrow{\varphi} G \xrightarrow{\psi} K \to 1$$

is a homomorphism $\sigma\colon K \to G$ such that $\psi \circ \sigma = \mathrm{id}_K$. If a splitting exists for a short exact sequence, then it is said to *split*.

Notice that if $\sigma\colon K \to G$ is a splitting, then σ is injective. To see this, consider $k \in K$. If $\sigma(k) = e_G$, then $\psi(\sigma(k)) = \psi(e_G) = e_K$. On the other hand, $\psi \circ \sigma = \mathrm{id}_K$, so $\psi(\sigma(k)) = k$. This shows that $k = e_K$.

3.18 THEOREM.

1. *If a short exact sequence $1 \to H \to G \to K \to 1$ splits, then G is isomorphic to a semidirect product $H \rtimes_\alpha K$.*
2. *If $G = H \rtimes_\alpha K$, then the short exact sequence $1 \to H \to G \to K \to 1$ splits.*

Proof. We first prove part 1. Consider a short exact sequence

$$1 \to H \xrightarrow{\varphi} G \xrightarrow{\psi} K \to 1,$$

with a splitting $\sigma\colon K \to G$. Note that σ and φ are injective homomorphisms, and so $\varphi(H)$ and $\sigma(K)$ are subgroups of G. Observe the following.

1. Since $\varphi(H) = \ker(\psi)$, we see that $\varphi(H) \trianglelefteq G$.
2. Let $g \in \varphi(H) \cap \sigma(K)$. If $g = \varphi(h) = \sigma(k)$ for some $h \in H$ and $k \in K$, then $e_K = \psi(\varphi(h)) = \psi(\sigma(k)) = k$. So $k = e_K$, and since σ is injective, we have $g = \sigma(e_K) = e_G$. Therefore $\varphi(H) \cap \sigma(K) = \{e_G\}$.
3. Let $g \in G$, and let $a = \sigma(\psi(g))$. Notice that

   $$\psi(\sigma(\psi(g))) = \psi(g).$$

   So $ga^{-1} \in \ker(\psi) = \operatorname{im}(\varphi) = \varphi(H)$. In this way we have

   $$g = (ga^{-1})(a) \in \varphi(H)\sigma(K),$$

   which shows that $G = \varphi(H)\sigma(K)$.

From the three observations above, we conclude that G is an internal semidirect product of $\varphi(H)$ and $\sigma(K)$. Since $H \cong \varphi(H)$ and $K \cong \sigma(K)$, we can say that G is isomorphic to a semidirect product of H and K.

More precisely, let us construct a homomorphism from K to $\operatorname{Aut}(H)$ that realizes G as a semidirect product of H and K. We know that the corresponding homomorphism from $\sigma(K)$ to $\operatorname{Aut}(\varphi(H))$ is described as

$$\sigma(k) \mapsto [\varphi(h) \mapsto \sigma(k)\varphi(h)\sigma(k)^{-1}].$$

We know that $K \cong \sigma(K)$ via the map $K \xrightarrow{\sigma} \sigma(K)$. Similarly, there is an isomorphism $\beta\colon \operatorname{Aut}(\varphi(H)) \to \operatorname{Aut}(H)$, described as follows. If $f \in \operatorname{Aut}(\varphi(H))$, then for any $h \in H$, set

$$(\beta(f))(h) = \varphi^{-1}(f(\varphi(h))).$$

In other words, $\beta = \varphi^{-1} \circ f \circ \varphi$. Now we construct a map $\alpha\colon K \to \operatorname{Aut}(H)$ as the following composition:

$$K \xrightarrow{\sigma} \sigma(K) \to \operatorname{Aut}(\varphi(H)) \xrightarrow{\beta} \operatorname{Aut}(H).$$

Concretely, if $k \in K$ and $h \in H$, then

$$\alpha_k(h) = \varphi^{-1}\left(\sigma(k)\varphi(h)\sigma(k)^{-1}\right).$$

We can now precisely show that $H \rtimes_\alpha K \cong G$, as follows. Define the map $\iota\colon H \rtimes_\alpha K \to G$ by $\iota((h,k)) = \varphi(h)\sigma(k)$. We check that ι is a homomorphism.

1. The map ι clearly sends the identity (e_H, e_K) to the identity e_G.

2. If (h_1,k_1) and (h_2,k_2) are elements of $H \rtimes_\alpha K$, then

$$\begin{aligned}(h_1,k_1)\cdot(h_2,k_2) &= (h_1\alpha_{k_1}(h_2), k_1k_2)\\ &= \left(h_1\varphi^{-1}\left(\sigma(k_1)\varphi(h_2)\sigma(k_1)^{-1}\right), k_1k_2\right).\end{aligned}$$

   So applying ι to the right hand side and using that φ is a homomorphism, we check that

$$\begin{aligned}\iota((h_1,k_1)(h_2,k_2)) &= \varphi(h_1)\sigma(k_1)\varphi(h_2)\sigma(k_1)^{-1}\sigma(k_1)\sigma(k_2)\\ &= \varphi(h_1)\sigma(k_1)\varphi(h_2)\sigma(k_2)\\ &= \iota((h_1,k_1))\iota((h_2,k_2)).\end{aligned}$$

   So ι distributes over products.

It is easy to check that ι is both injective and surjective (and hence an isomorphism). These arguments prove part 1 of the theorem.

Now we prove part 2 of the theorem. Suppose that $G = H \rtimes_\alpha K$. To show that the corresponding short exact sequence splits, we must demonstrate a splitting map $\sigma\colon K \to G$. Recall that the map $\psi\colon G \to K$ is the map $(h,k) \mapsto k$. Define $\sigma\colon K \to G$ to be the natural inclusion map $k \mapsto (e_H, k)$. It is clear that $\psi \circ \sigma = \mathrm{id}_K$, and therefore σ is a splitting of the short exact sequence. □

4 Classification of groups of certain orders

In this section we will show some examples of classifications of groups.

4.1 *Groups of order p and pq*

We already know that if p is a prime, then every group of order p is cyclic, and hence isomorphic to $\mathbb{Z}/p$.

We also know (from a homework problem) that if G a group of order p^2, then G is abelian. By the classification of finite abelian groups (which we will see later), we can retroactively deduce that G is either isomorphic to $\mathbb{Z}/p^2$ or $\mathbb{Z}/p \times \mathbb{Z}/p$.

Now suppose that $|G| = pq$, where p and q are distinct primes.

4.1 theorem. *Let $|G| = pq$ where p and q are distinct primes where $q > p$. Then G is isomorphic to a semidirect product $\mathbb{Z}/q \rtimes \mathbb{Z}/p$.*

Proof. We know that G has a Sylow p-subgroup K, as well as a Sylow q-subgroup H. The number of Sylow q-subgroups is a divisor of p that is congruent to 1 modulo q. Since $q > p$, the only possibility is that H is the unique Sylow q-subgroup. Therefore $H \trianglelefteq G$. We further observe the following.

1. Since $\gcd(p, q) = 1$, we must have $H \cap K = \{e_G\}$.
2. By the isomorphism theorems, we can write a formula for the size of HK:

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{qp}{1} = |G|.$$

   So $HK = G$.

Therefore $G \cong H \rtimes K$. But $H \cong \mathbb{Z}/q$ and $K \cong \mathbb{Z}/p$, so

$$G \cong \mathbb{Z}/q \rtimes \mathbb{Z}/p.$$

□

4.2 *Groups of (certain) small orders*

We first prove a useful lemma. This lemma states that if we modify a homomorphism $K \to \mathrm{Aut}(H)$ by precomposing by an automorphism of K, or postcomposing by a conjugation in $\mathrm{Aut}(H)$, then the semidirect product does not change up to isomorphism.

4.2 Lemma. *Let K and H be groups, and $\alpha\colon K \to \mathrm{Aut}(H)$ a homomorphism. Fix $\xi \in \mathrm{Aut}(H)$ and $\eta \in \mathrm{Aut}(K)$, and define $\alpha'\colon K \to \mathrm{Aut}(H)$ as*

$$\alpha'_k = \xi \circ \alpha_{\eta^{-1}(k)} \circ \xi^{-1}.$$

Then the two semidirect products $H \rtimes_\alpha K$ and $H \rtimes_{\alpha'} K$ are isomorphic.

Proof. Define a function $\mu\colon H \rtimes_\alpha K \to H \rtimes_{\alpha'} K$ by

$$\mu((h, k)) = (\xi(h), \eta(k)).$$

As a function, μ is a bijection. We now check that μ is a homomorphism.

1. Since ξ and η are homomorphisms, we know that $\mu((e_H, e_K)) = (e_H, e_K)$.
2. Suppose that (h_1, k_1) and (h_2, k_2) are two elements of $H \rtimes_\alpha K$. Then

$$(h_1, k_1) \cdot (h_2, k_2) = \left(h_1 \alpha_{k_1}(h_2), k_1 k_2\right).$$

   Applying μ to both sides, we see that

$$\mu((h_1, k_1) \cdot (h_2, k_2)) = \left(\xi(h_1)\xi(\alpha_{k_1}(h_2)), \eta(k_1)\eta(k_2)\right).$$

We can also compute that

$$\begin{aligned}\mu((h_1,k_1))\cdot\mu((h_2,k_2)) &= (\xi(h_1),\eta(k_1))\cdot(\xi(h_2),\eta(k_2))\\ &= \left(\xi(h_1)\alpha'_{\eta(k_1)}(\xi(h_2)),\eta(k_1)\eta(k_2)\right).\end{aligned}$$

Note that

$$\begin{aligned}\alpha'_{\eta(k_1)}(\xi(h_2)) &= (\xi\circ\alpha_{\eta^{-1}(\eta(k_1))}\circ\xi^{-1})(\xi(h_2))\\ &= \xi(\alpha_{k_1}(h_2)).\end{aligned}$$

So we see that

$$\begin{aligned}\mu((h_1,k_1))\cdot\mu((h_2,k_2)) &= \left(\xi(h_1)\xi(\alpha_{k_1}(h_2)),\eta(k_1)\eta(k_2)\right)\\ &= \mu((h_1,k_1)\cdot(h_2,k_2)).\end{aligned}$$

The above observations show that μ is a homomorphism. Since μ is clearly bijective, it is a group isomorphism, and we see that

$$H\rtimes_\alpha K\cong H\rtimes_{\alpha'}K.$$

□

Now we can classify groups of some small orders.

Orders 2, 3, 5, 7, etc

These are prime orders, so the groups must be $\mathbb{Z}/p$ for the appropriate prime.

Orders 4, 9, 25, etc

These are squares of primes, so the groups are either $\mathbb{Z}/p^2$ or $\mathbb{Z}/p\times\mathbb{Z}/p$. In class, we also classified all groups of order 4 "by hand".

Order 6

Since $6=2\times3$, we know that any group G of order 6 is a semidirect product $\mathbb{Z}/3\rtimes_\alpha\mathbb{Z}/2$. So now we classify all the distinct possibilities.

Note that for any $n\in\mathbb{N}$, we have $\mathrm{Aut}(\mathbb{Z}/n)\cong(\mathbb{Z}/n)^\times$, because any automorphism of $\mathbb{Z}/n$ can be specified uniquely by sending the generator $[1]_n$ to any $[m]_n$ such that m is invertible modulo n.

Let G be any group of order 6. Let H be the (unique) Sylow 3-subgroup in G and let K be any Sylow 2-subgroup in G. Let a be a generator of H and let b be a generator of K. So in particular, we have $\mathrm{Aut}(H)\cong\mathbb{Z}/2$. Any semidirect product is constructed by choosing a homomorphism $K\to\mathrm{Aut}(H)\cong\mathbb{Z}/2$. There are two possible homomorphisms.

The trivial homomorphism (which sends every $k \in K$ to $\mathrm{id}_H \in \mathrm{Aut}(H)$) gives us the "trivial" semidirect product, which is the direct product $H \times K$. In this case, $G \cong \mathbb{Z}/3 \times \mathbb{Z}/2 \cong \mathbb{Z}/6$.

The non-trivial homomorphism α sends $b \in K$ to the non-trivial automorphism of H, which sends a to a^2. We can easily check that in this case, $H \rtimes_\alpha K$ is nonabelian. For example,

$$(a,b)(a,e_K) = (a\alpha_b(a), b) = (a \cdot a^2, b) = (e_H, b),$$
$$(a,e_K)(a,b) = (a\alpha_{e_K}(a), e_K b) = (a^2, b).$$

So there is a unique nonabelian group of order 6. We already know that S_3 is a nonabelian group of order 6, so if α is nontrivial, we must have $G \cong S_3$.

Order 8

This is the first hard case, and we will not discuss the full classification here. Instead, we do some examples and state the classification. Recall that $D_{2\cdot 4}$ is a nonabelian group of order 8. It can be described as a subgroup of S_4 consisting of the following elements:

$$D_{2\cdot 4} = \{(1), (13), (24), (13)(24), (1234), (1432), (14)(23), (12)(34)\}.$$

We can check that the subgroup $\{(1), (13)(24)\}$ is normal in $D_{2\cdot 4}$, and that the quotient is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$. So we get a short exact sequence as follows.

$$1 \to \mathbb{Z}/2 \to D_{2\cdot 4} \to \mathbb{Z}/2 \times \mathbb{Z}/2 \to 1.$$

However, this sequence does not split — $D_{2\cdot 4}$ does not have any subgroup isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$ that has trivial intersection with $\{(1), (13)(24)\}$.

The *quaternion group* Q_8 is another nonabelian group of order 8. It is described as a set as follows:

$$Q_8 = \{1, -1, i, -i, j, -j, k, -j\}.$$

The relations are:

$$i^2 = j^2 = k^2 = -1,$$
$$ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik,$$
$$(-1)a = a(-1) \text{ for each } a \in Q_8.$$

Then the subgroup $\{1, -1\}$ is normal in Q_8, and the quotient is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$. Therefore we again have an exact sequence

$$1 \to \mathbb{Z}/2 \to Q_8 \to \mathbb{Z}/2 \times \mathbb{Z}/2 \to 1.$$

Once again, it can be checked that this exact sequence does not split.

Even though $D_{2\cdot 4}$ and $\cong Q_8$ fit into short exact sequences of the same shape, they are not isomorphic — for example, because $D_{2\cdot 4}$ has two elements of order 4, while Q_8 has six elements of order 4.

The complete and non-redundant list of groups of order 8 (up to isomorphism) is as follows:

$$\mathbb{Z}/8, \quad \mathbb{Z}/4 \times \mathbb{Z}/2, \quad \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2, \quad D_{2\cdot 4}, \quad Q_8.$$

Order 12

Let G be any group of order 12. Then G has a Sylow 3-subgroup (of order 3), and a Sylow 2-subgroup (of order 4).

4.3 Lemma. *Either G has a normal Sylow 3-subgroup or a normal Sylow 2-subgroup.*

Proof. If G has a normal Sylow 3-subgroup, we are done. Otherwise, G must have four Sylow 3-subgroups. Any two distinct Sylow 3-subgroups intersect trivially (because the intersection has a size that divides 3, but cannot be the full group). So the four Sylow 3-subgroups account for 9 distinct elements of G, including the identity.

We know that G has at least one Sylow 2-subgroup, which must intersect any Sylow 3-subgroup trivially (because $\gcd(3,4) = 1$). So the only possibility is that G has a unique Sylow 2-subgroup, consisting of the remaining three elements of G and the identity. So the Sylow 2-subgroup is normal. □

We use this lemma to carry out the classification.

Case 1: Suppose that H is the Sylow 2-subgroup, and that it is normal in G.

(a) If $H \cong \mathbb{Z}/4$, then $\mathrm{Aut}(H) \cong \mathbb{Z}/2$. There are no non-trivial maps from $\mathbb{Z}/3$ to $\mathbb{Z}/2$, so $G \cong \mathbb{Z}/4 \times \mathbb{Z}/3$.

(b) The other possibility is that $H \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. We can check that $\mathrm{Aut}(H) \cong S_3$. The trivial map $\mathbb{Z}/3 \to \mathrm{Aut}(H)$ gives us the direct product $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3$.
There are several nontrivial maps α from $\mathbb{Z}/3$ to $\mathrm{Aut}(H)$, obtained by sending the generator of $\mathbb{Z}/3$ to any 3-cycle in S_3. But any 3-cycle in S_3 is conjugate to any other 3-cycle, so any two nontrivial maps α and α' differ by a conjugation in $\mathrm{Aut}(H)$. By Lemma 4.2, any two semidirect products obtained from nontrivial maps α, α' are isomorphic. We already know that A_4 is a nonabelian group of order 12 that has $\mathbb{Z}/2 \times \mathbb{Z}/2$ as a normal subgroup. So if α is nontrivial, then G must be isomorphic to A_4.

Case 2: Suppose that H is the Sylow 3-subgroup, and that it is normal in G.
Let K be the quotient G/H. Note that $\mathrm{Aut}(H) \cong \mathbb{Z}/2$.

(a) Suppose that $K \cong \mathbb{Z}/4$. The trivial map $K \to \mathrm{Aut}(H)$ gives us the direct product $\mathbb{Z}/4 \times \mathbb{Z}/3$, which we have already considered. There is exactly one nontrivial homomorphism from $\mathbb{Z}/4$ to $\mathbb{Z}/2$, so there is at most one nontrivial semidirect product of this form. Let b be a generator of $K = \mathbb{Z}/4$ and let a be a generator of $H = \mathbb{Z}/3$. So we can describe the semidirect product $H \rtimes_\alpha K$ as

$$H \rtimes_\alpha K = \langle a, b \mid a^3 = b^4 = 1,\ ba = a^2 b \rangle.$$

(b) The other possibility is that $K \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. The trivial map $K \to \mathrm{Aut}(H)$ gives us the direct product $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3$, which we have considered already.
Let $\alpha \colon K \to \mathrm{Aut}(H)$ be a nontrivial map. It can be checked that $\mathrm{Aut}(K) \cong S_3$, and so any two nontrivial maps α differ by a precomposition by an element of $\mathrm{Aut}(K)$. So by Lemma 4.2, any two resulting semidirect products are isomorphic. We already know that $D_{2\cdot 6}$ is a nonabelian group of order 12. It has $\mathbb{Z}/3$ as a normal subgroup (the rotations by 120°) and $\mathbb{Z}/2 \times \mathbb{Z}/2$ as the quotient. So if α is nontrivial, then $H \rtimes_\alpha K$ must be isomorphic to $D_{2\cdot 6}$.

The classification is complete.

Order 15

Let G be any group of order 15. Recall that G must be isomorphic to a semidirect product $\mathbb{Z}/5 \rtimes \mathbb{Z}/3$. However, $\mathrm{Aut}(\mathbb{Z}/5) \cong \mathbb{Z}/4$, and there are no non-trivial homomorphisms from $\mathbb{Z}/3$ to $\mathbb{Z}/4$. So the only possibility is that $G \cong \mathbb{Z}/5 \times \mathbb{Z}/3 \cong \mathbb{Z}/15$.

5 Solvability and Jordan-Holder theorem

Lecture 10
September 19th, 2017
Notes by Jinsil Lee

5.1 *A solvable group*

5.1 definition. Assume that G is finite. The derived subgroup/commutator subgroup of a group G is a subgroup generated by all expressions $aba^{-1}b^{-1}$. And we denote $[G, G] = G'$.

5.2 observation. (i) $G' \lhd G$.

(ii) $G' = \{e\}$ iff G is abelian.

5.3 definition. A group G is called solvable if there is a finite normal series

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n \rhd \{e\}$$

such that G_i/G_{i+1} is abelian for each i in $\{0, \cdots, n\}$.

5.4 EXAMPLE. $G = S_4$

$$S_4 \triangleright A_4 \triangleright \mathbb{Z}_2 \times \mathbb{Z}_2 \triangleright \{e\}$$

And all successive quotients are abelian.

5.5 LEMMA. *If $\phi : G_1 \to G_2$ is a homomorphism then $\phi(G_1^{'}) < \phi(G_2^{'})$.*
In particular, if $G_1 < G_2$, then $G_1^{'} < G_2^{'}$.

Proof. Check on generators.

$$\phi(aba^{-1}b^{-1}) = \phi(a)\phi(b)\phi(a^{-1})\phi(b^{-1}) \in G_2^{'}.$$

□

5.6 LEMMA. *If $K \triangleleft G$ such that G/K is abelian, then $G^{'} < K$.*

Proof. Check on generators for G. And let $\Phi : G \to G/K$ be surjective homomorphism.

$$\Phi(aba^{-1}b^{-1}) = \Phi(a)\Phi(b)\Phi(a^{-1})\Phi(b^{-1}) = e_{G/K} \in G/K$$

It implies that $aba^{-1}b^{-1} \in K$. □

5.7 THEOREM. *The following are equivalent*

(i) *G is solvable*

(ii) *$G^{(n)}$ is abelian for some n*

(iii) *$G^{(k)}$ is $\{e\}$ for some k.*

Proof. $(ii) \Rightarrow (iii)$ take $k = n + 1$
$(iii) \Rightarrow (i)$ done.
$(i) \Rightarrow (iii)$ Assume G is solvable. Then there exists a normal series

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n \triangleright \{e\}$$

such that G_i/G_{i+1} is abelian for all i. Since G/G_1 is abelian, $G^{'} < G_1$. By induction, assume that for some k, $G^{(k)} < G_k$. We know G_k/G_{k+1} is abelian. By lemma 1.6, we thus see that $G_k^{'} < G_{k+1}$. Moreover, $(G^{(k)})^{'} < G_k^{'} < G_{k+1}$ by lemma 1.5. It follows that $G^{(k+1)} < G_{k+1}$. By induction, $G^{(k)} < G_k$ for all k.
By previous claim, we know $G^{(n+1)} < G_{n+1} = \{e\}$. Thus, we can conclude that $G^{(n+1)} = \{e\}$. □

5.8 COROLLARY. *If $H < G$ and G is solvable, then H is solvable.*

Proof. $H^{(n)} < G^{(n)}$. Since G is solvable, $G^{(n)} = \{e\}$ for some n. We conclude that $H^{(n)} = \{e\}$ for some n. □

5.9 corollary. *If there exists a surjective map ϕ from G to $H^{'}$ and if G is solvable, then H is solvable.*

5.10 corollary. *If $K \triangleleft G$ and both K and G/K are solvable, then G is solvable.*

Proof. If $\Phi : G \to G/K$, then $\Phi : G^{(n)} \to (G/K)^{(n)}$ for all n. Let n be such that $(G/K)^{(n)} = \{e\}$. Then $\Phi : G^{(n)} \to \{e\}$ which implies that $G^{(n)} < K$. Choose k such that $K^{(k)} = \{e\}$. Therefore, $G^{(n+k)} < \{e\}$, so $G^{(n+k)} = \{e\}$. We conclude that G is solvable. □

5.11 theorem. *If G is a p-group (i.e. $|G| = p^k$ for some prime p), then G is solvable.*

Proof. If $k \leq 2$ then G is abelian, so that G is solvable.
If $k \geq 3$ then G has a subgroup of order p^{k-1} by sylow theorem I. It is normal by homework and its quotient is abelian.
Now use induction. If $|G| = p^k$, then $Z(G) \neq \{e\}$ by class equation. And $Z(G) \triangleleft G$. If $Z(G) = G$, then G is abelian and then it is solvable. Since $G/Z(G)$ and $Z(G)$ are both p-groups of smaller order, they are solvable by using induction. Corollary 1.10 implies that G is solvable. □

5.2 *A non-solvable group*

5.12 definition. G is simple if G has no normal subgroups other than $\{e\}$ and G.

5.13 observation. (i) Note that $[G, G] = G^{'} \triangleleft G$
If G is simple, $G^{'} = \{e\}$ or $G^{'} = G$.

(ii) If $G^{'} = \{e\}$ i.e. G is abelian, then G is simple. $\iff$ $G \cong \mathbb{Z}/p\mathbb{Z}$ for some prime p.

(iii) If G is not abelian, G is simple $\iff$ $G^{'} = G$. $\Rightarrow$ Simple, nonabelian groups are not solvable.

5.14 example. A_5 is simple.

Proof. Use class equation of A_5. $(1) \in A_5, (123) \in A_5, (12)(34) \in A_5, (12345) \in A_5$. And $|A_5| = \frac{5!}{2} = 60$. A_5 has no non-trivial normal subgroup. □

5.15 theorem. *If $n \geq 5$, then A_n is not solvable.*

Proof. $A_5 < A_n$ if $n \geq 5$. If A_n were solvable, then A_5 would have been solvable. □

$\Rightarrow S_n$ is not solvable for $n \geq 5$.

5.16 theorem. *(Jordan-Hölder-Theorem) If $n \geq 5$, then A_n is simple.*

5.3 *Simplicity of A_n*

Lecture 11
September 26th, 2017
Notes by Joseph Dorta

Returning to our Example 5.14 in which we proved that A_5 is simple, we note some key observations.

5.17 observation. A_5 has:

- 1 one-cycle,
- 15 2-2-cycles $e.g. cycles of the form (12)(34)$
- 20 3-cycles,
- 24 5-cycles.
- For 3-cycles $|S_5| = 120$ and there are 20 3-cycles all of which are conjugate by elements of S_5. Notice that the stabilizer of any given 3-cycle has order 6, namely $|Stab_{(123)}S_5| = 120/20 = 6$. More explicitly $Stab_{(123)}S_5 = \{1, (123), (132), (123)(45), (132)(45)\}$. Where we note that $(123)(45)$ and $(132)(45)$ are not in A_5, hence $|Stab_{(123)}A_5| = 3$. Now $|A_5| = 60$ so that $|Orbit((123))$ in $A_5| = 20$ which means that the 3-cycles are also all conjugate in A_5.
- Consider the 5-cycles, choose (12345), and we proceed as before to compute its orbit and stabilizer in S_5. We know from previous work that all 5-cycles are conjugate in S_5, so that $|Stab_{(12345)}S_5| = 120/24 = 5$. Note that (12345) and all of it's powers, of which there are 5, stabilize the element (12345) hence $Stab_{(12345)}$ ={powers of (12345)}= $Stab_{(12345)}A_5$ since each 5-cycle is an element of A_5. Then applying the orbit-stabilizer theorem to A_5, we have $|Orbit_{(12345)}$in $A_5| = 60/5 = 12$. From this we immediately note that not all 5-cycles are conjugate in A_5. Similar to the 3-cycles, the 2-2 cycles are all conjugate in A_5.
- By the class equation $|A_5| = 60 = 1 + 12 + 12 + 15 + 20$. Where we note that none of these combinations of conjugacy classes add up to a divisor of A_5 other than $id = (e)$ and A_5 itself. Hence, the only normal subgroups of A_5 are the trivial ones.

5.18 theorem. 1. *A_n is not solvable for $n \geq 5$.*

2. *A_n is simple for $n \geq 5$.*

The proof of part 2 of the theorem can be found in Jacobson's Basic Algebra.

5.19 theorem. ***Jordan-Holder Theorem***

1. *If G is a finite group, then G has a normal series $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \ldots \triangleright G_n \triangleright 1$ such that $G_{i+1} \triangleleft G_i$, $G_{i+1} \neq G_i$ and G_i/G_{i+1} is simple for each i. Such a series is called a Jordan-Holder series or a composition series.*

2. *If $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \ldots \triangleright G_n$ and $G = H_0 \triangleright H_1 \triangleright H_2 \triangleright \ldots \triangleright H_n$ are two composition series, then $m = n$ and there is a permutation σ of $\{0, 1, 2, ..., n\}$ such that $H_i/H_{i+1} \cong G_i/G_{i+1}$. The G_i/G_{i+1} are called composition factors.*

5.20 observation. G_1 is a maximal proper normal subgroup of G_0 and G_{i+1} is a maximal proper normal subgroup of G_i, so that G_i/G_{i+1} will be simple.

Part II: Ring theory

6 Rings

6.1 definition. A *ring* R is an Abelian group with respect to addition $(R, +, 0)$ together with the associative binary operation $\cdot : R \times R \to R$ such that $\cdot$ has the following properties:

1. R is a monoid under $\cdot$, i.e. R has a multiplicative identity $r \cdot 1 = 1 \cdot r = 1$ for all $r \in R$.
2. Distributivity: For all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

6.2 definition. A ring R is *commutative* if $\cdot : R \times R \to R$ is commutative.(Note that + is always commutative).

6.3 examples. 1. $(\mathbb{Z}, +, \cdot, 0, 1)$

2. $(\mathbb{R}, +, \cdot, 0, 1)$
3. $(\mathbb{C}, +, \cdot, 0, 1)$
4. $(\mathbb{Q}, +, \cdot, 0, 1)$
5. $(\mathbb{Z}_n, +, \cdot, \overline{0}, \overline{1})$
6. The Gaussian Integers $(\mathbb{Z}[i], +, \cdot, 0, 1)$ defined by $\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\}$ with usuual complex addition and multiplication. Note that *mathbbZ*$[i]$ is a subring of $\mathbb{C}$.
7. $M_{n\times n}(\mathbb{C}) = \{n \times n$ matrices with entries in $\mathbb{C}\}$, where the 0 additive identity element is the matrix with a 0 in every entry and the 1 multiplicative identity is the $n \times n$ identity matrix with $1's$ on its diagonal and $0's$ for every other entry. Note that this ring is not commutative since it is not always that case that $AB = BA$.

Rings in general need not necessarily have multiplicative inverses. In particular, it can happen that $a, b \in R$ wit $a \neq 0, b \neq 0$ and $ab = 0$. In this case, a and b are called **zero divisors**.

6.4 example.
- In $\mathbb{Z}_6, \overline{2} \cdot \overline{3} = \overline{0}$ and $\overline{2}, \overline{3} \neq \overline{0}$.
- In $M_{n\times n}(\mathbb{C})$ we have $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = 0$. Note that in the non-commutative case, we can specify left and right zero divisors. In the example above $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is a right zero divisor.

- If R has no zero divisors, it is called a *domain*.
- If $R - \{0\}$ forms a group under $\cdot$, then R is called a *division ring*.
- A commutative division ring is called a *field*. For example, $\mathbb{R}, \mathbb{Z}, \mathbb{Q}, \mathbb{Z}_p$ where p is a prime.

6.5 example. **Quaternions**

- We define the quaternions as $:= \{a + bi + jc + kd | a, b, c, d \in \mathbb{R}\}$ with the rules that $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j$ and the coefficients in $\mathbb{R}$ commute with i, j, k. Note that $\mathbb{H}$ is a non-commutative division ring.
- If G is an group under $\cdot$ and $\mathbb{F}$ is any field then define $\mathbb{F}_G = \{\mathbb{F} - linearcombinationsofelementsofG\}$. To with, if $g_1, g_2 \in G$, then $3g_1 + 2g_2 \in \mathbb{F}_G$. Note that if $e \in G$ is the identity element of G, then $1 \cdot e = e$ is the multiplicative identity element of $\mathbb{F}_G$. This construction $\mathbb{F}_G$ is called the *group ring*.
- If R_1, R_2 are rings, then $R_1 \times R_2$ is a ring with additive identity $(0, 0)$ and multiplicative identity $(1, 1)$. Note that if R_1, R_2 are not the zero rings, then $R_1 \times R_2$ always has zero divisors. For example $(a, 0) \cdot (0, b) = (0, 0)$.
- The quaternions can also be presented as

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -b & \bar{a} \end{pmatrix} \middle| a, b \in \mathbb{C} \right\}$$

  We have the following correspondence between the two presentations: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \leftrightarrow 1$, $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \leftrightarrow i$, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \leftrightarrow j$, $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \leftrightarrow k$.
  If $\mathbb{H}_1$ is our first presentation and $\mathbb{H}_2$ is the second, then we claim that $\mathbb{H}_1 \cong \mathbb{H}_2$ as rings.

6.6 definition. A map $\phi : R_1 \to R_2$ is a *ring homomorphism* if:

1. $\phi(0_{R_1}) = 0_{R_2}$
2. $\phi(1_{R_1} = 1_{R_2}$
3. $\phi(a + b) = \phi(a) + \phi(b)$
4. $\phi(ab) = \phi(a)\phi(b)$

ϕ is an*isomorphism* if there is an inverse homomorphism $\psi : R_2 \to R_1$ such that $\psi = \phi^{-1}$

Now let R be any commutative ring; we introduce $M_{n\times n}(R) = \{n \times n$ matrices with entries in $R\}$. We also have the map det: $M_{n\times n}(R) \to R$ which is a monoid homorphism for $\cdot$ since $det(AB) = det(A)det(B)$ but note that $\det(A+B) \neq \det(A) + \det(B)$. Recall that $GL_n(R)$ is the group of $n \times n$ invertible matrices with entries in R, so that $M_{n\times n}(R) \supset GL_n(R)$ and the det homomorphism restricted to $GL_n(R)$ maps to the invertible elements of R under $\cdot$, to wit $\phi(GL_n(R) \subset U(R)$.

Lecture 12
October 3rd, 2017
Notes by Keneth Allen

6.7 proposition. *If R is a division ring, then any subring is a domain.*

Proof. $r \cdot s \neq 0$ in the subring if r, s are non-zero because r and s are invertible as elements of R. □

Partial converse: If D is any domain, does it embed in a division ring? In other words, is there a division ring R such that $D \hookrightarrow R$ is a subring?

Answer: No if D is non-commutative (Example in Jacobson-Malcev).

If D is commutative, then there is always at least one commutative division ring that contains D as a subring.

6.1 *Fraction Field Construction:*

Let D be a commutative domain. Define $Frac(D) = \{(a,b)|a \in D, b \in D^\times\}$ where $(a,b) \sim (c,d)$ if $ad = bc$.

Addition: $[(a,b)] + [(c,d)] = [(ad+bc, bd)]$

Multiplication: $[(a,b)] \cdot [(c,d)] = [(ac, bd)]$

Additive identity: $[(0,1)] = [(0,a)], a \neq 0$.

Multiplicitive identity: $[(1,1)] = [(a,a)], a \neq 0$.

$[(a,b)] = "\frac{a}{b}"$

Remark: Need to check $+, \cdot$ are well-defined.

6.8 theorem. *$Frac(D)$ is a field (commutative division ring) and $D \hookrightarrow Frac(D)$.*

Proof. Let $[(a,b)] \in Frac(D)$, such that $a \neq 0$. $\Rightarrow [(a,b)] \cdot [(b,a) = [(ab, ab)] = [(1,1)]$

$D \to Frac(D)$

$r \mapsto [(r,1)]$ is an injective map of rings. □

6.2 *Localization of a commutative domain at a multiplicitive set S:*

Example: $Frac(\mathbb{Z}) = \mathbb{Q} \supset \{\frac{a}{b} \in \mathbb{Q} | b = 2^n, n \in \mathbb{N}_0\}$, a subring of $\mathbb{Q}$ containing $\mathbb{Z}$.

6.9 definition. Let $S \subset R$ be a subset not containing 0. Then S is called a multiplicitive set if $a, b \in S \Rightarrow ab \in S$

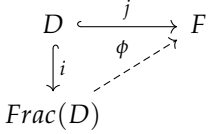
In the case $Frac(\mathbb{Z}) = \mathbb{Q}, S = \mathbb{Z}^\times$.
In the case $\{\frac{a}{b} \in \mathbb{Q}, b = 2^n, n \in \mathbb{N}\}, S = 2^n$.

6.10 DEFINITION. The localization $S^{-1}D = \{(a,b)|a \in D, b \in S\}/\sim$ where $(a,b) \sim (c,d)$ if $ad = bc$

This is a ring under $+$ and $\cdot$ as defined previously.

6.3 *Universal Property of* Frac(D)

Suppose F is a field, such that $j : D \hookrightarrow F$ is an injective. Then there is a unique injective map $i : Frac(D) \to F$ such that:



commutes.

Proof. Define ϕ as follows:
$\phi([(a,b)]) = j(a)j(b)^{-1}$
Check well-defined map of rings:
$\phi([(ac,bc)]) = j(ac)j(bc)^{-1} = j(a)j(c)j(b)^{-1}j(c)^{-1} = j(a)j(b)^{-1}$
Also, $\phi \circ i = j$
$(\phi \circ i)(a) = \phi([(a,1)]) = j(a)j(1)^{-1} = j(a)$
To prove this map is unique, Suppose that ϕ_1 and ϕ_2 are two maps with this property. Then $(\phi_1 \circ i) = j = (\phi_2 \circ i)$, and we want to show that $\phi_1 = \phi_2$.
Let $a \in D$
Then $(\phi_1 \circ i)(a) = \phi_1[(a,1)] = (\phi_2 \circ i)(a) = \phi_2([(a,1)])$
So $\phi_1 = \phi_2$ on elements of the form $[(a,1)]$.
Let $b \in D^\times$. Check that $\phi_1([(1,b)]) = \phi_2([(1,b)])$. This implies $\phi_1[(a,1)] \cdot \phi_1([(1,b)]) = \phi_2([(a,1)]) \cdot \phi_2([(1,b)]). \Rightarrow \phi_1([(a,b)]) = \phi_2([(a,b)])$. □

6.4 *Polynomial Rings*

All rings are commutative for this section. Suppose $R \subset S$ a subring and $s \in S$.

6.11 DEFINITION. $R[s]$ is the smallest subring of S containing R and s.

6.12 EXAMPLE. $\mathbb{Q} \supset \mathbb{Z}[\frac{1}{2}] = \{\frac{a}{b}|b = 2^n\}$

6.13 DEFINITION. The one-variable polynomial ring $R[x] = \{r_0, r_1, r_2, ...|r_i \in R, \exists N, r_n = 0 \forall n > N\}$

Addition is component wise. Multiplication: $(r_0, r_1, ...)(s_0, s_1, ...) = (\sum_{i=1}^{n} r_i s_{n-i})_n$.
"0" $= (0,0,0,0,...)$
"1" $= (1,0,0,0,...)$

"x" $= (0, 1, 0, 0, ...)$

This is a commutative rings and its elements can be written as $\sum_i r_i x^i$ which is a finite sum.

6.14 proposition. $R \hookrightarrow R[x]$

6.15 theorem. *Let $R \subset S$ subring, and $s \in S$. Then there is a unique ring homomorphism $R[x] \to R[s]$, such that:*

$$\begin{array}{ccc} R & \xrightarrow{\ j\ } & R[s] \\ {\scriptstyle i}\downarrow & \nearrow_{\phi} & \\ R[x] & & \end{array}$$

commutes and $x \mapsto s$. Further, the map $R[x] \to R[s]$ is surjective.

Proof. Define ϕ by, $\phi((r_0, r_1, ...)) = \sum_i r_i s^i$. Notice that ϕ must be unique because we must have that $\phi(1) = 1$ and $\phi(x) = s$, and so $\phi(x^i) = s^i$. Also as defined, ϕ is a ring homomorphism.

Notice: $im(\phi)$ contains R and $im(\phi)$ contains s, so $im(\phi) \subset R[s]$ is a subring of S containing both R and s, so $im(\phi) = R[s]$. i.e. ϕ is surjective, so $R[x] \twoheadrightarrow R[s]$. So by the first issomorphism theorem of rings: $R[s] \cong R[x] \backslash (Ker\phi)$ □

6.16 definition. If $ker\phi$ is trivial, the s is said to be transcendental over R. Otherwise, s is said to be algebraic.

6.17 example. $\mathbb{Q} \hookrightarrow \mathbb{R}$ For $\mathbb{Q}[e], \phi$ has trivial kernel. (Assuming we know e is transcendental). An element $\sum_i r_i x^i \in Ker\phi \iff \sum_i r_i s^i = 0$ in s.

6.18 definition. $R[x_1, x_2] = (R[x_1])[x_2]$

6.19 theorem. *If $\sigma \in S_n$, then the rings $R[x_1, ..., x_n] \cong R[x_{\sigma(1)}, ..., x_{\sigma(n)}]$*

Polynomial rings over fields and PIDs

Lecture 13
October 5th, 2017
Notes by Sergio E. Garcia Tapia

Beyond this point, all rings considered will be commutative. Recall that last time we defined, given a ring R, the polynomial ring $R[x]$, and inductive also define

$$R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}]$$

which is the ring of polynomial with n variables.

6.20 theorem. *If $\pi \in S_n$, then there is a unique isomorphism*

$$R[x_1, x_2, \ldots, x_n] \cong R[x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}]$$

that sends $x_i \to x_i$. Furthermore, there are surjections

$$R[x_1, \ldots, x_n] \twoheadrightarrow R[x_1, \ldots, x_{n-1}]$$

by sending $x_n \to 0$ (by sending $x_n \to r \in R$).

6.21 remark. If $S = R$, then certainly $R \subset S$. Given $u \in S$, then $R[u] = R$, for it is certainly the smallest ideal containing R and u. We have the map

$$R[x] \twoheadrightarrow R[u] = R$$

by sending x to u. It is called the "evaluation map ev_u."

One-variable polynomial rings: $R[x]$

If $f(x) \in R[x]$, wen can write

$$f(x) = \sum_{i=1}^{n} a_i x^i, \quad a_i \neq 0.$$

Then the following terminology will be useful

- $\deg(f(x)) = n$, and if R is an integral domain, then given $g(x) \in R[x]$, we have

  $$\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x)).$$

  Note that if R was not an integral domain, there would be zero divisors and it could well be the case that multiplying the leading coefficient of $f(x)$ and of $g(x)$ could give 0, and this expression for the degree of their product would not be true.

- The leading coefficient of $f(x)$ is a_n.

- For the zero polynomial, we have $\deg(0) = -\infty$ by convention.

6.22 theorem. *Let R be a domain. Then the units of $R[x]$ are just the units of R.*

Proof. Suppose that $f(x) \in R[x]$ is a unit. Then there exists a polynomial $g(x) \in R[x]$ such that $f(x) \cdot g(x) = 1$. But the degree of a constant polynomial is 0, so

$$0 = \deg(1) = \deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x)).$$

This means that $\deg(f(x)) = \deg(g(x)) = 0$, so $f(x)$ is a unit of R. □

6.23 theorem. *Let R be a domain. Let $f(x), g(x) \in R[x]$, such that $g(x) \neq 0$, $m = \deg(g(x))$, and b_m is the leading coefficient of $g(x)$. Then there exists a $k \in \mathbb{N}_0$,*

and some $q(x), r(x) \in R[x]$ *with the property that* $\deg(r(x)) < m$ *and*

$$b_m^k f(x) = g(x)q(x) + r(x).$$

An immediate corollary of this is the following.

6.24 corollary. *If* R *is a field, we have*

$$f(x) = g(x)q(x) + r(x)$$

for some $q(x), r(x) \in R[x]$ *such that* $\deg(r(x)) < m$.

The proof of this corollary is simply by dividing through by b_m^k. Now we prove the theorem.

Proof. Let $n = \deg(f(x))$. We will use induction on n to obtain the result. For the base case, we take $n < m$. If $n < m$, we can set $q(x) = 0$, $r(x) = f(X)$, and $k = 0$. Now suppose that $n \geq m$, and set

$$f_1(x) := b_m f(x) - a_n x^{n-m} g(x).$$

In doing this, we are canceling the leading coefficients of $f(x)$ and $g(x)$, so the $\deg(f_1(x)) < n$, allowing us to use induction. By the case we proved, there exists $k \in \mathbb{N}_0$ such that

$$b_m^k f_1(x) = g(x)q(x) + r(x)$$

where $\deg(r_1(x)) < m$, and substituting back in

$$b_m^k(b_m f(x) - a_n x^{n-m} g(x)) = g(x) - q_1(x) + r_1(x)$$

$$b_m^{k+1} f(x) = g(x) \underbrace{(g_1(x) + b_m^k a_n x^{n-m})}_{q(x)} + \underbrace{r_1(x)}_{r(x)}.$$

□

6.25 remark. If b_m is a unit, then we can write

$$f(x) = g(x) + b_m^{-k} g(x)q(x) + r(x)$$

so without loss of generality we can say

$$f(x) = g(x)q(x) + r(x).$$

This $q(x)$ and $r(x)$ in this expression are unique. If we also had $f(x) =$

$g(X)q_1(x) + r_1(x)$, then we could equate and substract to get

$$r(x) - r_1(x) = g(x)(q_1(x) - q(x))$$

and because the of the left-handside is less than the degree of the right-handside if $q_1(x) \neq q(x)$ (because they are being multiplied by $g(x)$, which satisfies $\deg(g(x)) > \deg(r(x))$), it must be the case that $r_1(x) = r(x)$ and $q_1(x) = q(x)$.

6.26 theorem. *If $f(x) \in R[x]$ and $a \in R$, then $(x - a)$ divides $f(x)$ if and only if $f(a) = 0$*

Proof. Write $f(x) = (x - a)q(x) + r(x)$. □

6.27 theorem. *Let F be a field. Then $F[x]$ is a Principal Ideal Domain (PID). That is, every ideal in $F[x]$ is generated by a single element.*

Proof. Certainly it holds for the 0 ideal, since (0) is an ideal. So we assume that $I \subset F[x]$ is a nonzero ideal. Let $g(x) \neq 0$ be an element of I of minimal degree. We will show that the ideal I is generated by $g(x)$. If $f(x) \in I$, then

$$f(x) = g(x)q(x) + r(x).$$

Since $\deg(r(x)) < \deg(g(x))$, and since $r(x) = f(x) - g(x)q(x)$, the fact that I is an ideal implies $r(x) \in I$. But $\deg(r(x)) < \deg(g(x))$, and since $g(x)$ is the minimum degree nonzero polynomial, we must have $r(x) = 0$, so that $f(x) = g(x)q(x)$ and hence $f(x) \in (g(x))$. □

6.28 example. Consider $\mathbb{Z}[x]$. This is not a PID, because

$$(2, x) \subset \mathbb{Z}[x]$$

is not principal, as you should verify.

Recall that the map $\varphi : F[x] \twoheadrightarrow F[u]$, and $I = \ker \varphi$. Then

$$F[u] \cong F[x]/I,$$

and by the result just proved, $I = (g(x))$ for some $g(x) \in F[x]$. As briefly mentioned last time,

- If $g(x) = 0$, then u is called transcendental over F.
- If $g(x) \neq 0$, then u is algebraic over F. Now assume that $g(x)$ is a monic polynomial, which means that the leading coefficient is 1 (otherwise, the fact that we are in a field allows us to divide through by it). Then $g(x)$ is called the minimal polynomial of u over F.
- Since $g(x)$ generates the $\ker \varphi$, we certainly have $g(u) = 0$.

- g is the monic polynomial of minimal degree such that $g(u) = 0$.

6.29 remark. If $M \in M_n(\mathbb{C})$, then there is a polynomial $p(x)$ of degree n such that $p(M) = 0$. Namely,

$$p(x) = \det(xI - M).$$

However, the minimal polynomial of M could have smaller degree. Let $R = \mathbb{C}$, and let $S = M_n(\mathbb{C})$. Then $R \subset S$, since we have the map

$$r \to \begin{bmatrix} r & & \\ & \ddots & \\ & & r \end{bmatrix}$$

If $M \in S$, thne we can consider $\mathbb{C}(M) \subseteq S$, and the map

$$\varphi : \mathbb{C}[x] \twoheadrightarrow \mathbb{C}[M] \cong \mathbb{C}[x]/(g(x)),$$

where $\ker \phi = I = (g(x))$. Then $g(x)$ is the minimal polynomial of M.

6.30 theorem. *Let u be algebraic over F, so that*

$$F[u] \cong F[x]/(g(x)), \quad g(x) \neq 0.$$

1. *If there are no polynomials $h_1(x)$ and $h_2(x)$ with $\deg(h_i(x)) > 0$ such that $g(x) = h_1(x)h_2(x)$, then we say that $g(x)$ is irreducible. In this case, $F[u]$ is a field.*
2. *If $g(x)$ is reducible, then $F[u]$ is not a domain.*

Because we can prove this theorem, we need the following Lemma.

6.31 Lemma. *Let $I \subset R$ be an ideal. Every ideal R/I is of the form J/I for some ideal J in R that contains I.*

Proof. Exercise. □

Now we prove the theorem.

Proof. 1. Let's calculate the ideals of $F[u]$. We shall take $J \subset F[x]$ and take $J/(g(x))$. Let J be an ideal in $F[x]$ that contains $(g(x))$. We know that $J = (f(x))$ for some $f(x) \in F[x]$ and that $g(x) \in J$. Therefore,

$$g(x) = f(x)h(x)$$

for some $h(x) \in F[x]$. Since $g(x)$ is irreducible by assumption, it must be that $\deg(f(x)) = 0$ or $\deg(h(x)) = 0$. If $\deg(f(x)) = 0$, then $f(x) \in F$

and $(f(x)) = (1)$ (the unit ideal, which is $F[x]$). If $\deg(h(x)) = 0$, then $h(x) \in F$ and $(g(x)) = (f(x))$. Therefore we either have

$$J = (g(x)) \quad \text{or} \quad J = (g(x)).$$

If $J = (1)$, then

$$J/(g(x)) \cong F[x]/(g(x)) = F[u],$$

or if $J = (g(x))$, then

$$J/(g(x)) = (0).$$

So $F[u]$ has exactly two ideals, and it is commutative, so it is a field.

2. For the second part, let $g(x) = h_1(x)h_2(x)$. Then $\deg(h_i(x)) > 0, h_1(u), h_2(u)$ are nonzero in $F[u]$, and $h_1(u)h_2(u) = g(u) = 0$, so we have zero divisors and hence $F[u]$ is a domain in this case.

□

6.32 example. Let $g(x) = x^2 + 1 \in \mathbb{R}[x]$. It is irreducible over $\mathbb{R}[x]$ and

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}.$$

6.33 theorem. *Let $f(x) \in F[x]$. Then if $n = \deg(f(x))$, then $f(x)$ has at most n distinct roots in F.*

6.34 example. $\mathbb{Z}/6 \cong \mathbb{Z}/2 \times \mathbb{Z}/3$, and $f(x) = x(x+1)$ has 4 roots: $0, 2, 3, 5$.

Lecture 14
October 10th, 2017
Notes by Freddy Saia

We now prove the above theorem:

Proof. By induction on k, we will show that if $r_1, \ldots, r_k$ are distinct roots of $f(x)$, then

$$\prod_{i=1}^{k}(x - r_k) \mid f(x).$$

Beginning with the base case of $k = 1$, if r_1 is a root of $f(x)$ then $f(r_1) = 0$. We proved previously that this implies that $(x - r_1) \mid f(x)$. Suppose that the result holds for all $k < n$. Since r_1 is a root of $f(x)$, we again have $(x - r_1) \mid f(x)$ such that

$$f(x) = f_1(x)(x - r_1)$$

for some $f_1(x) \in F[x]$. For any $i \in \{2, \ldots, k\}$, we get

$$0 = f(r_i) = f_1(r_i)(r_i - r_1).$$

Since $r_i \neq r_1$ by assumption, it follows that r_i is a root of $f_1(x)$. Our induction hypothesis then implies that

$$\prod_{i=2}^{k}(x - r_i) \mid f_1(x),$$

from which it immediately follows that

$$\prod_{i=1}^{k}(x - r_i) \mid f(x).$$

This fact we have proven, combined with the fact that the degree of a product of polynomials over a domain is equal to the sum of their degrees, concludes the proof. □

6.35 COROLLARY. *If F is a field and G is a finite, multiplicative subgroup of $F \setminus \{0\}$, then G is cyclic.*

Proof. Suppose G is such a subgroup of $F^\times$ for a field F. Recall that the exponent $e(G)$ of G is defined to be the smallest $m \in \mathbb{N}$ such that $x^m = 1$ for all $x \in G$. It is a quick consequence of Lagrange's Theorem that $e(G) < |G|$, and in fact $e(G) = |G|$ if and only if G is cyclic. As $x^{e(G)} = 1$ for all $x \in G$, this polynomial over F has at least $|G|$ distinct roots. The previous theorem therefore implies that $e(G) \geq |G|$. Hence, it must be the case that $e(G) = |G|$ □

6.36 EXAMPLE. For p a prime, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

6.5 *Unique factorization domains*

6.37 DEFINITION. For D a commutative domain, we have the following definitions:

- $r \in D$ is a factor of $s \in D$ if there exists some $r' \in D$ such that $s = rr'$. In this case, we write $r \mid s$.
- $u \in D$ is called a unit if $u \mid 1$, i.e. if u is an invertible element of D.
- r is a proper factor of s if $r \mid s$ but $s \nmid r$.

- a non-zero, non-unit r is irreducible in D if r cannot be expressed as $r = s_1 s_2$, where s_1 and s_2 are both proper factors of r (it follows that s_1, s_2 are not units).

- r_1, r_2 are associates if $r_1 \mid r_2$ and $r_2 \mid r_1$. Equivalently, there exists some unit $u \in D$ such that $r_1 = u r_2$. We write $r_1 \sim r_2$ to denote that r_1 and r_2 are associate.

- $p \in D$ is prime if $p \mid ab$ implies that $p \mid a$ or $p \mid b$ for any $a, b \in D$.

These definitions allow us to state what we mean by (unique) factorizations in a commutative domain D:

6.38 definition. An element $r \in D$ has a factorization (into irreducibles) if there are finitely many irreducibles $p_1, p_2, \ldots, p_n \in D$ such that

$$r = \prod_{i=1}^{n} p_i.$$

This factorization is said to be essentially unique if for any other such factorization of r into irreducibles

$$r = \prod_{i=1}^{m} q_i,$$

it is the case that $m = n$ and that there is some $\pi \in S_n$ such that $p_i \sim q_{\pi(i)}$ for each $i = 1, \ldots, n$.

This leads to the following definition of a special kind of commutative domain:

6.39 definition. A commutative domain D is a unique factorization domain (UFD) if every non-zero, non-unit in D has an essentially unique factorization into irreducibles.

We now explore some properties of UFDs:

6.40 proposition. *A UFD D satisfies the descending chain condition (dcc) on factors, i.e. if there is a sequence $\{r_i\}_{i \in \mathbb{N}}$ such that $r_{i+1} \mid r_i$ for all $i \in \mathbb{N}$, then there is some $N \in \mathbb{N}$ such that $r_m \sim r_{m+1}$ for all $m \geq N$.*

Proof. The proof of this proposition is left as an exercise. □

6.41 proposition. *If D is a UFD, then any irreducible in D is also prime.*

Proof. Let D be a UFD and $p \in D$ an irreducible element. Suppose that $a, b \in D$ such that $p \mid ab$, so we have some $d \in D$ such that

$$pd = ab.$$

Irreducibles cannot be units by definition, so a and b cannot both be units. We may then write

$$\begin{aligned} a &= p_1 p_2 \cdots p_r u_1 \\ b &= q_1 q_2 \cdots q_s u_2, \end{aligned}$$

where each p_i and q_j is prime, both u_1 and u_2 are units in D, and at least one of these factorizations is non-trivial (i.e. at least one of r or s is at least 1). The product $pd = ab$ then has (essentially) unique factorization

$$pd = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s u_1 u_2.$$

By unique factorization in D, it must then be the case that $p \sim p_i$ or $p \sim q_j$ for some i or j, proving that $p \mid ab$. Since the product ab was arbitrary, this shows that p is prime. □

6.42 example. Here is a non-example: in $\mathbb{Z}[\sqrt{-5}]$, we have

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

It can be checked that the factors in the above equation are all irreducibles in this ring (for example, by defining

$$\begin{aligned} N : \mathbb{Z}[\sqrt{-5}] &\to \mathbb{N}_0 \\ a + b\sqrt{-5} &\mapsto a^2 + 5b^2 \end{aligned}$$

and showing that this function is multiplicative.) However, we can see concretely from the above equation that they are not prime. The previous proposition therefore implies that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

The next theorem states that the previous two properties of UFDs, combined, are actually sufficient for a ring to be a UFD:

6.43 theorem. *A domain D is a UFD if and only if*

(1) D satisfies the dcc on factors, and

(2) every irreducible element in D is prime.

Proof. We have already shown that if a domain is a UFD, then it satisfies the two properties of the theorem. We now prove the converse. Suppose that D is a domain satisfying the two properties of the theorem. For any nonzero non-unit $a \in D$, we must show that it has a factorization into irreducibles, which is essentially unique.

Let $a \in D$ be a nonzero non-unit. First we show that a has at least one irreducible factor. If $a = a_1$ is itself irreducible, then it is its own irreducible factor. Otherwise, a has a proper factor a_2. Again, if a_2 is irreducible, then we are done. Inductively, we check that if a_i is not irreducible, we can find a proper factor a_{i+1}. But D satisfies the *dcc* on factors, so we can't have an infinite descending sequence of proper factors. Consequently, a_i is irreducible for some $i \in \mathbb{N}$, and it is an irreducible factor of a.

Now we show that a has a factoring into irreducibles. Choose an irreducible factor p_1 of a, so that $a = p_1 b_1$. For each b_i, we inductively construct b_{i+1} by choosing an irreducible factor p_{i+1} of b_i (if it exists), such that $b_i = p_{i+1} b_{i+1}$. Notice that if b_i has an irreducible factor p_{i+1}, then b_{i+1} is necessarily a proper factor of b_i. So we get an infinite descending chain of factors b_i, such that b_{i+1} is a proper factor of b_i unless b_i is a unit. Since D satisfies *dcc* on factors, it must be the case that b_i is a unit for some i. So we get

$$a = p_1 p_2 \cdots p_{i-1}(p_i b_i),$$

which is a factorization of a into irreducibles. This argument proves that every nonzero non-unit $a \in D$ has a factorization into irreducibles.

Now we show that such a factorization is essentially unique. Suppose that $a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$ be two factorizations into irreducibles. Suppose WLOG that $m \geq n$.

Since $p_1 \mid q_1 \dots q_n$ and p_1 is irreducible (and hence prime), we see that $p_1 \mid q_i$ for some i. Rearrange factors if necessary so that $p_1 \mid q_1$. Since q_1 is irreducible, we have $p_1 \sim q_1$. We can now cancel p_1 and q_1 so that

$$p_2 p_3 \cdots p_m = u_1 q_2 \cdots q_n,$$

for some unit u_1. Similarly, we show by induction (and up to reordering) that $p_i \sim q_i$ for each $i \leq n$. So we can now write

$$p_{n+1} \cdots p_m = u_1 u_2 \cdots u_n$$

for units $u_1, u_2, \dots, u_n$. The irreducible p_m cannot divide a product of units, which shows that $m = n$. We have already shown that each p_i is associate to q_i for each i, and so the factoring is essentially unique. □

6.6 *Euclidean domains*

Having defined UFDs and PIDs, we define and investigate another special type of integral domain. We will soon learn that these notions are all related.

6.44 DEFINITION. A commutative domain D is a Euclidean domain if there exists a function

$$\delta : D \setminus \{0\} \to \mathbb{N}$$

such that for all $a \in D$ and $b \in D \setminus \{0\}$ there exist $q, r \in D$ such that

$$a = bq + r \quad \text{with } \delta(r) < \delta(b).$$

6.45 EXAMPLE. Let's consider some examples of Euclidean domains with corresponding Euclidean maps δ:

- The integers: $\mathbb{Z}$, with $\delta(n) = |n|$, can easily be checked to be Euclidean.
- The Gaussian integers: $\mathbb{Z}[i]$ with $\delta(a + bi) = a^2 + b^2$. Note that this δ is just the square of the complex absolute value function. We now prove that this is in fact a Euclidean domain:

Lecture 15
October 12th, 2017
Notes by Terrin Warren

Proof. Let $a, b \in \mathbb{Z}[i]$ with $b \neq 0$. Then we want to find some $q, r \in \mathbb{Z}[i]$ such that $a = bq + r$ where $\delta(b) < \delta(r)$. First we define the closest integer function for $\mathbb{Q}[i]$. Recall that if $\alpha \in \mathbb{Q}$, then $\|\alpha\|$ is the integer such that $|\|\alpha\| - \alpha| \leq \frac{1}{2}$.

If $\alpha + \beta i \in \mathbb{Q}[i]$, then we define $\|\alpha + \beta i\|$ to be $\|\alpha\| + \|\beta\| i$ in $\mathbb{Z}[i]$. Suppose $\frac{a}{b} \in \mathbb{Q}[i]$, then let $\frac{a}{b} = \mu + \nu i$ and consider $\|\frac{a}{b}\|$. This gives us the following, $\|\frac{a}{b}\| = \|\mu\| + \|\nu\| i$. So $a = b(\|\mu\| + \|\nu\| i) + b(\epsilon + \eta i)$, where $\epsilon = \mu - \|\mu\|$, and $\eta = \nu - \|\nu\|$.

Let $q = \|\mu\| + \|\nu\| i$ and $r = b(\epsilon + \eta i) = a - b(\|\mu\| + \|\nu\| i)$. Then observe that $q, r \in \mathbb{Z}[i]$ and $\delta(r) = |b|^2(\epsilon^2 + \eta^2) \leq |b|^2(\frac{1}{4} + \frac{1}{4}) = \frac{1}{2}|b|^2 = \frac{1}{2}\delta(b) < \delta(b)$. □

Now we return our attention to the more general unique factorization domains, let D be a UFD.

6.46 DEFINITION. Let $a, b \in D$, where a, b can be written as follows: $a = u \cdot p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}$ and $b = v \cdot p_1^{n_1} \cdot p_2^{n_2} \cdots p_r^{n_r}$ where u, v are units in D and p_i is irreducible in D. Then we defind the $\gcd(a, b) = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$, where $k_r = \min(m_r, n_r)$.

6.47 THEOREM. *If $e \in D$ such that $e|a$ and $e|b$, then $e|\gcd(a, b)$.*

The proof of this theorem follows from the difinition of gcd if we write e as a product of irriducibles.

6.7 *Polynomial extensions of UFDs*

6.48 theorem. *If D is a UFD, then $D[x]$ is a UFD. In fact, inductively, we also have that $D[x_1, x_2, \ldots, x_r]$ is a UFD.*

In order to prove this theorem, we want to show that $D[x]$ satisfies:

1. dcc for factors and
2. every irrecucible in $D[x]$ is prime.

In order to prove that the first condition is satisfied, it is useful to consider the gcd of the coefficients of some given $f(x) \in D[x]$. Before we prove the second condition, we should first consider the following lemma.

6.49 Lemma. *If $d \in D$ and $d|a(x)b(x)$, then either $d|a(x)$ or $d|b(x)$.*

Proof. Suppose $a(x) = \sum_{i=0}^{m} a_i x^i$ and $b(x) = \sum_{i=0}^{n} b_i x^i$. If $d|a_m b_n$, then $d|a_m$ or $d|b_n$ since d is prime in D. If $d|a_m$ and $d|b_n$, then we can eliminate the top degree terms from $a(x)$ and $b(x)$ and consider these instead.

Assume without loss of generality that $d \nmid a_m$ and $d|b_n$. Then the coefficient of x^{m+n-1} in the product of $a(x)b(x)$ is $a_m b_{n-1} + a_{m-1} b_n$. Then since $d|a_m b_{n-1} + a_{m-1} b_n$ and $d|b_n$ implies that we must also have that $d|a_m b_{n-1}$. But $d \nmid a_m$, so $d|b_{n-1}$. Inductively, we can check that $d|b_i$ for all i. Thus, $d|b(x)$. □

Proof. of 6.48

1. Suppose we have a descending chain $f_1(x), f_2(x), \ldots$ such that $f_{i+1}(x)|f_i(x)$ for all $i \in \mathbb{N}$. Let d denote the gcd of the coefficients of $f_1(x)$. Then $d = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$ for some irreducible elements $p_i \in D$. Now suppose for sake of contradiction that dcc is not satisfied for this descending chain. This means that there does not exist an $N \in \mathbb{N}$ such that for all $n > N, f_{n+1}(x) \sim f_n(x)$, i.e. $f_{n+1}(x)$ is a proper factor of $f_n(x)$ for all $n \in \mathbb{N}$.

   We can extract a subsequence from the chain such that $g_{i+1}(x)$ is a proper factor of $g_i(x)$. Let $\beta(g_i(x)) = \deg(g_i(x)) + \sum_{j=2}^{r} k_{ij}$ where the gcd of the coefficients of $g_i(x)$ is given by $d_i = p_1^{k_{i_1}} \cdot p_2^{k_{i_2}} \cdots p_r^{k_{i_r}}$. Then because this is a subsequence from the descending chain, we have that $d_i|d$. Given that $g_{i+1}(x)$ is a proper factor of $g_i(x)$, we have that $\beta(g_{i+1}(x)) < \beta(g_i(x))$ since either the degree of the polynomial or the gcd of the coefficient must decrease as we move down the chain. This gives us a contradiction since β is always positive and takes on integer values meaning that the subsequence of $g_i(x)$'s cannot be infinite. Then there must be some

$N \in \mathbb{N}$ such that for all $n > N$, $f_{n+1}(x) \sim f_n(x)$ and so $D[x]$ satisfies the dcc as desired.

2. Let $f(x) \in D[x]$ be irreducible. Then the gcd of the coefficients of $f(x)$ is 1 since it is irreducible. Suppose that $f(x)|a(x)b(a)$ for some $a(x), b(x) \in D[x]$. Then we can write a generalized division statement: $c^k a(x)b(x) = f(x)g(x)$ where c is the leading coefficient of $f(x)$ and $k \geq 1$. Then $c|f(x)g(x)$ where $c = p_1 \cdot p_2 \cdots p_r$ where each p_i is an irreducible element of D. So we must have that $p_i|f(x)g(x)$ for all i. Then lemma 6.49 implies that either $p_i|f(x)$ or $p_i|g(x)$. We know that $p_i \nmid f(x)$ because the gcd of the coefficients of $f(x)$ is 1, and each p_i is a factor of the leading coefficient of $f(x)$. So it must be the case that $p_i|g(x)$ for all i. Then we can cancel each p_i successively, which gives up $a(x)b(x) = f(x)g_1(x)$ where $g_1(x) = \frac{1}{c^k}g(x)$. Suppose $a(x) = \prod a_i(x)$ and $b(x) = \prod b_i(x)$ as a product of irreducibles. Then $f(x)$ is irreducible implies that $f(x) \sim a_i(x)$ or $f(x) \sim b_i(x)$ for some i. Thus $f(x)|a(x)$ or $f(x)|b(x)$.

□

6.50 theorem.

1. *If F is a field, then $F[x]$ is a Euclidian domain.*
2. *Every Euclidian domain is a PID.*
3. *Every PID is a UFD.*

Part III: Galois theory

Lecture 16
October 17th, 2017
Notes by Jinsil Lee

7 Field automorphisms

We already know that $\mathbb{Q}$ and $\mathbb{Z}/p\mathbb{Z}$ for p a prime. A field automorphism is just a ring isomorphism from a field to itself.

7.1 theorem. *Any field automorphism of $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ is the identity.*

Proof.

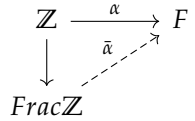
7.2 remark. If R is any ring then there exist a unique ring homomorphism from $\mathbb{Z}$ to R.

Case of $\mathbb{Q}$ Let $\phi : \mathbb{Q} \to \mathbb{Q}$ be an automorphism. Then we know that $\phi(0) = 0, \phi(1) = 1$ and ϕ is an isomorphism. It follows that $\phi(-1) = -1$ and then $\phi(n) = n$ and $\phi(-n) = -n$ for any $n \in \mathbb{N}$ by induction. Moreover, if $n \neq 0$ is in $\mathbb{Z}$, $\phi(\frac{m}{n})\phi(n) = \phi(\frac{m}{n}n) = \phi(m)$. Therefore, $\phi(\frac{m}{n})\phi(n)^{-1} = mn^{-1} = \frac{m}{n}$. So $\phi = id_{\mathbb{Q}}$.

Case of $\mathbb{F}_p$ Let $\phi : \mathbb{F}_p \to \mathbb{F}_p$ be an automorphism. Then it follows that $\phi(\bar{0}) = \bar{0}, \phi(\bar{1}) = \bar{1}$ and $\phi(\bar{n}) = \bar{n}$ by induction. So $\phi = id_{\mathbb{F}_p}$. □

Let F be a field. There exists a ring homomorphism $\alpha : \mathbb{Z} \to F$ where $\alpha(1) = 1_F$. Consider $ker\alpha \subset \mathbb{Z}$ an ideal. $ker\alpha = (0)$ or $ker\alpha = (n)$ for some $n \in \mathbb{N}$.

7.3 definition. The characteristic of F is the number $n \geq 0$, such that $ker\alpha = (n)$. If char F= o, it means that the inclusion map $\alpha : \mathbb{Z} \to F$ is injective. Hence, There exists a unique injection from $\mathbb{Q}$ to F by universial properties of fraction fields because it's a ring map of fields.



7.4 remark. Suppose char $F = n > 0$. Then n is prime. Suppose $n = ab$ where $a, b > 1$. Then we get $0 = \alpha(n) = \alpha(a)\alpha(b)$ in F. We conclude that either $\alpha(a) = 0$ or $\alpha(b) = 0$ which contradict to the fact that n is the generator of $ker\alpha$. So n must be prime.

7.5 exercise. If $charF = p$, then there exists a unique injection from $\mathbb{F}_p toF$.

7.6 theorem. *If $\phi : \mathbb{R} \to \mathbb{R}$ is a field homomorphism, then ϕ is the identity.*

Proof. Suppose that $\phi : \mathbb{R} \to \mathbb{R}$ is a field homomorphism. Then ϕ must be injective. Consider $\phi|\mathbb{Q} : \mathbb{Q} \to \mathbb{R}$. By previous arguments, $\phi|\mathbb{Q} = id_{\mathbb{Q}}$. Let $x \in \mathbb{R}$ and $x > 0$. This means $x = y^2$ for some $y \in \mathbb{R}$. So, $\phi(x) = \phi(y^2) = \phi(y)^2 > 0$. So if $x > 0$, then $\phi(x) > 0$. If $u > w (u - w > 0)$, then $\phi(u - w) > 0$ and $\phi(u) > \phi(w)$. So ϕ is order preserving.

Let $x \in \mathbb{R}$. Then there exist sequences $\{p_n\}, \{q_n\}$ such that $\{p_n\}$ is increasing sequence and converges to x and $\{q_n\}$ is a decreasing sequence and converges to x. So $p_n = \phi(p_n) \leq \phi \leq \phi(q_n = q_n$ for each $n \in \mathbb{N}$ since $p_n, q_n \in \mathbb{Q}$. Use lub/glb properties of $\mathbb{R}$ to conclude that $\phi(x) = x$. □

It is hard to analyze automorphisms of $\mathbb{C}$. We deal with the easier case that $\phi : \mathbb{C} \to \mathbb{C}$ that preserve $\mathbb{R}$, that is, if $x \in \mathbb{R} \subset \mathbb{C}$, then $\phi(x) \in \mathbb{R} \subset \mathbb{C}$.(not necessarily pointwise!)

7.7 theorem. *If $\phi : \mathbb{C}/\mathbb{R} \to \mathbb{C}\mathbb{R}$ is an automorphism preserving $\mathbb{R}$, then $\phi(z) = z$ or $\phi(z) = \bar{z}$ for any z.*

Proof. If $z \in \mathbb{C}$, $z = x + iy$ for $x, y \in \mathbb{R}$. Since $\phi(i)^2 = -1$, $\phi(i) = i$ or $\phi(i) = -i$. If $\phi(i) = i$, $\phi(x + iy) = x + iy$ for any $x, y \in \mathbb{R}$. If $\phi(i) = -i$, $\phi(x + iy) = x - iy$ for any $x, y \in \mathbb{R}$. □

Let $F \subset E$ be a subfield of a field E (written E/F). E can be thought of as a vector space over F, so it has a dimension as an F-vector space and it has bases as F-vector space.

7.8 example. $\mathbb{C}$ is a 2-dim $\mathbb{R}$-vs with basis $1, i$.

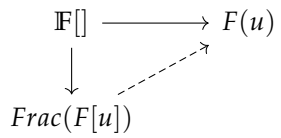
7.9 definition. If $F \subset E$, then $\dim_F E = [E : F]$ =degree of the field extension.

7.10 example ($\mathbb{R}$:$\mathbb{Q}$). $=\infty$

7.11 definition. Let $F \subset E$ and let $u \in E$. Then $F(u)$ = smallest subfield of E containing F and u.

Compare $F(u)$ with $F[u]$. Recall there exists a unique surjection $\alpha : F[x] \to F[u]$ sending $x \to u$. $ker\alpha = (f(x)) \subset F[x]$ is an ideal. We divide into two cases.
Case 1: $f(x) \neq 0$ [u is algebraic /F].
Note $f(x)$ is not a unit, because $\alpha \neq 0$. Claim that $f(x)$ is irreducible. If $f(x)$ us reducible, then $F[x]/(f(x))$ is not a domain but $F[u]$ is a domain because it is subring of E, a field. Look at $F[x]/(f(x)) \cong F[u]$. So in this case, $F[u]$ is already a field since $f(x)$ is irreducible/ F. So $F[u] = F(u)$. Then $f(u) = 0$ and f is minimal polynomial of u over F. $F[u]/F$ has a finite basis/ F and then $\{1, u, \cdots, u^{n-1}\}$ where $n = deg(f)$. So $[F[u] : F] = n = deg(f(x))$.
Case 2: $f(x) = 0$ (In this case, u is transcendental over F.)
u doesn't have a minimal polynomial /F. $F[u]$, as an F-vector space, has the following (infinite) basis $\{1, u, \cdots, \}$. $F[u] \neq F(u)$ in this case. Suppose not, so

$F[u] = F(u)$. So $u^{-1} \in F[u]$ and $u^{-1} = a_0 + a_1 u + a_2 u^2 + \cdots a_n u^n$. It follows that $a_n u^{n+1} + a_{n-1} u^n + \cdots a_0 u - 1 = 0$. This is a contradiction. Then there exists a unique map extending $F[u]$ to $F(u)$.



But $Frac(F[u])$ is subfield containing F and u. So $F(u) \subset Frac(F[u])$.

7.12 THEOREM. *If u is transcendental /F, then* $F(u) = Frac(F[u]) = \{\frac{f(u)}{g(u)} | g(u) \neq 0\}$. $[F(u) : F]$ *is infinite.*

7.13 EXAMPLE. $\mathbb{Q}[x] \neq \mathbb{Q} = Frac(\mathbb{Q}[x])$

7.14 THEOREM. *Let* $F \subset E \subset K$ *be field extensions such that* $[K : F] < \infty$. *Then* $[K : F] = [K : E][E : F]$.

Proof. Let $a = [K : E]$ and $b = [E : F]$. We can take $\{k_1, \cdots, k_a\}$ as a basis of K/E and $\{e_1, \cdots, e_b\}$ as a basis of E/F. Show that $\{k_i e_j\}$ is a basis of K/F. □

Lecture 17
October 19th, 2017
Notes by Jack Wagner

8 Constructibility

Let $S_1 = \{P_1, P_2, \ldots, P_n\}$ where each P_j is a point in the plane. We can define an inductive procedure to construct S_{i+1} given S_i where S_{i+1} consists of the following points:

1. Intersection points of all lines joining pairs of points from S_i.
2. Intersections of these lines with circles having centers in S_i and radius of length $|Q_m Q_n|$ for $Q_m, Q_n \in S_i$.
3. Intersections of all pairs of circles defined in the (2).
4. All points of S_i.

Using this procedure, define the constructible set $C(P_1, \ldots, P_n) = \bigcup_{i=1}^{\infty} S_i$.

8.1 EXAMPLE. If $S_1 = \{P\}$, then all steps are trivial and $C(P) = \{P\}$.

We will show that if $|S_1| \geq 2$, then $C(P_1, \ldots, P_n)$ is dense in the plane $\mathbb{R}^2$.

Assume that $|S_1| \geq 2$, and $P_1 = 0$ and $P_2 = 1$. We can consider points as lying in the complex plane. Suppose that $W_1, W_2 \in C(P_1, \ldots, P_n)$. Construct $w_1 + w_2$ by intersecting the circle with center at w_1 and radius $|w_2|$ with the circle with center at w_2 and radius $|w_1|$.

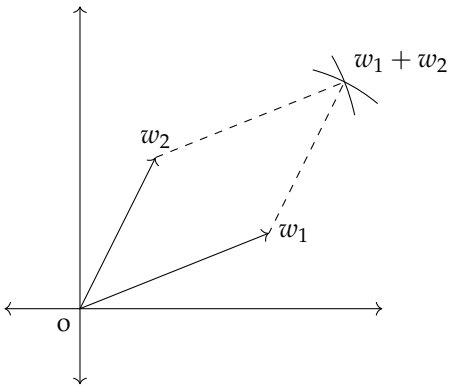


Figure 2: construction of $w_1 + w_2$

We can construct $-w_1$ by reflecting. That is, intersect the circle centered at 0 with radius w_1 with the line through 0 and w_1. They will intersect at w_1 and $-w_1$.

Recall that $\arg(w_1 w_2) = \arg(w_1) + \arg(w_2)$, and that $|w_1 w_2| = |w_1||w_2|$. Thus, in order to construct $w_1 w_2$, it is sufficient to show that we can copy angles and construct the length $|w_1 w_2|$. Showing that we can copy angles is left as an exercise. In order to construct $|w_1 w_2|$, consider the triangle with vertices 0, 1, and w_1. We can construct a similar triangle with base $|w_2|$ by copying angles. This new triangle has a side with length $|w_1 w_2|$.

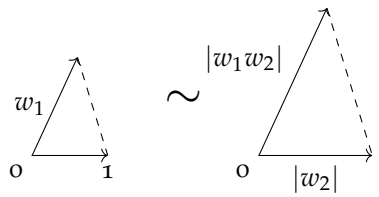


Figure 3: Using similar triangles to construct $|w_1 w_2|$

Thus, if $w_1, w_2 \in C(P_1, \ldots, P_n)$, then $w_1 \pm w_2 \in C(P_1, \ldots, P_n)$ and $w_1 w_2 \in C(P_1, \ldots, P_n)$. Therefore, $C(P_1, \ldots, P_n)$ is a subring of $\mathbb{C}$. Furthermore, if $w_2 \neq 0$, then $\frac{1}{w_2} \in C(P_1, \ldots, P_n)$ using a similar construction as the previous.

This proves the following theorem:

8.2 theorem. *If $n \geq 2$, and $P_1 = 0$ and $P_2 = 1$, then $C(P_1, P_2, \ldots, P_n)$ is a subfield of $\mathbb{C}$.*

The next natural question to answer is if $C(P_1, P_2, \ldots, P_n) = \mathbb{C}$. If it is not,

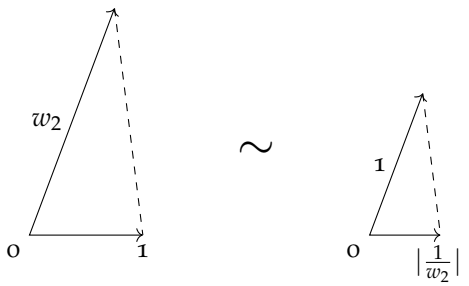


Figure 4: Constructing $\frac{1}{w_2}$ using similar triangles

what is it? To answer these, let us explore other operations we can do in $C(P_1, P_2, \ldots, P_n)$.

1. Complex conjugation

   If $w \in C(P_1, P_2, \ldots, P_n)$, then we can construct $\overline{w}$ by first constructing the line through w perpendicular to the line through 0 and 1. The proof that we can do this is left as an exercise. The circle centered at 0 with radius $|w|$ will intersect that line at w and $\overline{w}$. Thus, $\overline{w} \in C(P_1, P_2, \ldots, P_n)$.

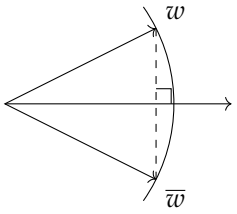


Figure 5: Constructing the complex conjugate

2. Square roots

   Recall that if $w \in C(P_1, P_2, \ldots, P_n)$, then $\arg(\sqrt{w}) = \frac{1}{2}\arg(w)$ and $|\sqrt{w}| = \sqrt{|w|}$. Thus, to show that $\sqrt{w} \in C(P_1, P_2, \ldots, P_n)$, we need to show that we can bisect angles take square roots of real lengths.

   Let l be the line through 0 and 1, and let l_w be the line through 0 and w. In order to bisect the angle formed between these two lines, intersect these lines with the circle with center 0 and radius $|w|$. This line will intersect l_w at w, and l at some point, P. Now intersect the circles with centers w and P and radius $|w|$. The line through 0 and this intersection will bisect the angle.

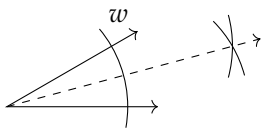


Figure 6: Bisecting an angle

If r is a real length, then we can construct a segment with length $\sqrt{r}$ in the following way: from the point 1, construct a segment of length r away from 0, making a segment with length $r+1$. Construct a circle whose diameter is that segment, and a line through 1 perpendicular to the segment. The distance between the point 1 and the intersection of the line with the circle will have length $\sqrt{r}$.

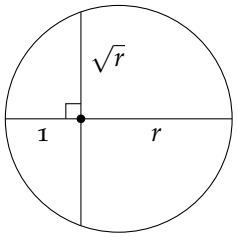


Figure 7: Segment with length $\sqrt{r}$

Combining these, we get that $\sqrt{r} \in C(P_1, P_2, \ldots, P_n)$.

8.3 theorem. *$C(P_1, \ldots, P_n)$ is the smallest subfield of $\mathbb{C}$ which contains $P_1, \ldots, P_n$, and is closed under complex conjugation and square roots.*

Proof. We have already shown that $C(P_1, \ldots, P_n)$ is a subfield of $\mathbb{C}$ which contains $P_1, \ldots, P_n$, and is closed under complex conjugation and square roots.

Let C' be any subfield of $\mathbb{C}$ with the desired properties. We will show that $C' \supset C(P_1, \ldots, P_n)$.

First, notice that if $x, y \in \mathbb{R}$ where $x + iy \in C'$, then $x - iy \in C'$. By adding and subtracting these, we get that $2x \in C'$, and $2iy \in C'$. Because $1 \in C'$, we know that $2 \in C'$. Thus, $\frac{1}{2} \in C'$, and so $\frac{1}{2}2x = x \in C'$. Similarly, $iy \in C'$. Because $-1 \in C'$, and C' is closed under square roots, $\sqrt{-1} = i \in C'$. Thus, $y \in C'$. This gives us that $x + iy \in C'$ if and only if $x, y \in C'$.

Suppose we have two points in C'. We can create a line joining them, $ax + by + c = 0$, where $a, b, c \in C'$.

Let $P, Q_1, Q_2 \in C'$, where $Q_1 = (q_1, r_1)$, and $Q_2 = (q_2, r_2)$. Because $|Q_1Q_2| = \sqrt{(q_2 - q_1)^2 + (r_2 - r_1)^2}$, we know that $|Q_1Q_2| \in C'$. Thus, the circle

with center P and radius $|Q_1Q_2|$ can be written as $x^2 + y^2 + dx + ey + f = 0$ where $d, e, f \in C'$. Let us look at the possible intersections.

1. Intersect 2 lines

   If $ax + by + c = 0$, and $a'x + b'y + c' = 0$ are both lines with coefficients in C', then the intersection will have coordinates in C' by Cramer's Rule.

2. Line and a circle

   If $ax + by + c = 0$ and $x^2 + y^2 + dx + ey + f = 0$ both have coefficients in C', then the intersections will be in C'. This is because we can solve for either x or y in the line, and substitute into the circle. From there, finding the intersection comes down to finding solutions of a quadratic equation. Since C' is closed under square roots, the solutions will be in C'.

3. 2 circle

   If $x^2 + y^2 + dx + ey + f = 0$ and $x^2 + y^2 + d'x + e'y + f' = 0$ both have coefficients in C', then subtracting them yields $(d - d')x + (e - e')y + f - f' = 0$. This reduces to the case of a line and a circle, so the intersection is contained in C'.

Because C' is closed under the possible intersections between lines and circles, and C' contains $P_1, P_2, \ldots, P_n$, we get that $C \supset C(P_1, \ldots, P_n)$. □

8.4 REMARK. We have shown that $C(P_1, \ldots, P_n)$ contains all numbers of the form $p + iq$ where $p, q \in \mathbb{Q}$. Because $\mathbb{Q}^2$ is dense in $\mathbb{R}^2$, we get that $C(P_1, \ldots, P_n)$ is dense in $\mathbb{R}^2$.

8.5 THEOREM. *Let $z_1, \ldots, z_n \in \mathbb{C}$. Set $F = \mathbb{Q}(z_1, \ldots, z_n, \overline{z_1}, \ldots, \overline{z_n})$.*

A number $z \in bbC$ is constructible from $0, 1, z_1, \ldots, z_n$ if and only if there is a finite sequence $u_1, u_2, \ldots, u_r \in \mathbb{C}$ such that

1. *$u_i^2 \in F(u_1, \ldots, u_{i-1})$ for all i,*
2. *$z \in F(u_1, \ldots, u_r)$.*

8.6 REMARK. Such an extension $F(u_1, \ldots, u_r)$ is called a square root tower.

Proof. Let $C' = \{z \in \mathbb{C} | z$ lies in some square root tower over $F\}$.

We'll show that $C' = C(0, 1, \ldots, z_n)$.

If $w_1, w_2 \in C'$, then $w_1 \in F(u_1, \ldots, u_r)$, and $w_2 \in F(v_1, \ldots, v_s)$. Because, $F(u_1, \ldots, u_r) \subset F(u_1, \ldots, u_r, v_1, \ldots, v_S)$, and $F(v_1, \ldots, v_s) \subset F(u_1, \ldots, u_r, v_1, \ldots, v_S)$, we get that $w_1, w_2 \in F(u_1, \ldots, u_r, v_1, \ldots, v_S)$, which is a field. Thus, $w_1 \pm w_2 \in C'$, and $w_1 w_2 \in C'$.

If $z \in C'$, then $z \in F(u_1, \ldots, u_r)$. This gives us that $\sqrt{z} \in F(u_1, \ldots, u_r, \sqrt{z})$, and so C' is closed under square roots. Furthermore, $\overline{z} \in \overline{F(u_1, \ldots, u_r)} = F(\overline{u_1}, \ldots, \overline{u_r})$. Therefore, C' is closed under complex conjugation.

Because C' is a field that is closed under complex conjugation and square roots, we get that $C' \supset C(0, 1, z_1, \ldots, z_n)$.

If $z \in C'$, then $z \in F(u_1, \ldots, u_r)$. Notice that $u_1^2 \in F$, and $F \subset C(0, 1, z_1, \ldots, z_n)$. Because $C(0, 1, z_1, \ldots, z_n)$ is closed under square roots, $u_1 \in C(0, 1, z_1, \ldots, z_n)$. Continuing inductively, we get that $F(u_1, \ldots, u_r) \subset C(0, 1, z_1, \ldots, z_n)$ for any square root tower, so $C' \subset C(0, 1, z_1, \ldots, z_n)$. □

Lecture 18
October 24th, 2017
Notes by Nolan Schock

Let $C = C(0, 1)$ denote the Euclidean constructible numbers. We will now focus on the problem of angle trisection. We know that we can construct two lines with a 60° degree angle between them. We aim to answer the following question: can we construct a 20° angle, trisecting the angle of the aforementioned lines?

If the answer is yes, then $\cos 20^\circ \in C$. Let $\theta = 20^\circ$. We know that

$$\cos(3\theta) = \cos(60^\circ) = 1/2 = 4\cos^3(\theta) - 3\cos(\theta).$$

Let $\alpha = \cos\theta$. Then

$$8\alpha^3 - 6\alpha - 1 = 0.$$

This implies that α and 2α are both algebraic over $\mathbb{Q}$: α is a root of the polynomial $8x^3 - 6x - 1$, and 2α is a root of the polynomial $x^3 - 3x - 1$.

If $x^3 - 3x - 1$ factors over $\mathbb{Q}$, then it factors over $\mathbb{Z}$ by Gauss' lemma. But if there exists a root of $x^3 - 3x - 1$, then by the rational root theorem it must divide -1, so it must be ± 1. But neither of these are roots of $x^3 - x - 1$, so we conclude that the polynomial is irreducible over $\mathbb{Q}$, and hence it is the minimal polynomial for 2α. Therefore,

$$[\mathbb{Q}(2\alpha) : \mathbb{Q}] = 3.$$

But if $2\alpha \in C$, then 2α would lie in a square root tower over $\mathbb{Q}$. However, square root towers have degree 2^k for some k. Thus looking at the tower of extensions

$$\mathbb{Q} \to \mathbb{Q}(2\alpha) \to \mathbb{Q}(u_1, \ldots, u_r),$$

where $\mathbb{Q}(u_1, \ldots, u_r)$ is a root extension of degree 2^k over $\mathbb{Q}$, the tower law implies that

$$2^k = [\mathbb{Q}(u_1, \ldots, u_r) : \mathbb{Q}(2\alpha)]3,$$

a contradiction. Thus $2\alpha \notin C$, so $\alpha \notin C$.

9 Galois theory

Let $F \subseteq E$ be a field extension. Ultimately, we want to study the group

$$\mathrm{Aut}(E/F) = \{\varphi : E \to E \mid \varphi \text{ is a field automorphism such that } \varphi(a) = a \text{ for all } a \in F\}.$$

We are mainly concerned with the case where $F \subseteq E$ is an algebraic extension.

9.1 *Splitting fields*

9.1 definition. Let $f(x) \in F[x]$. A *splitting field* E for $f(x)$ over F is an extension of F such that

1. There exist $r_1, \ldots, r_n \in E$ such that

   $$f(x) = (x - r_1) \cdots (x - r_n)$$

   in $E[x]$.

2. $E = F(r_1, \ldots, r_n)$, i.e. E is the smallest extension of F in which $f(x)$ splits.

9.2 theorem. *If $f(x) \in F[x]$ is monic of degree n, then there is a splitting field E of $f(x)$ over F.*

Proof. First notice that $F \subseteq F[x]$. Write $f(x) = f_1(x) \cdots f_k(x)$, where each f_i is monic and irreducible over F. If each f_i is already linear, then $E = F$ is a splitting field of $f(x)$ over F, and we are done.

We now proceed by "downward induction" on the number of factors k of $f(x)$.

Base Case: If $k = n$, then we are done by the above discussion.

Inductive Step: Suppose $k < n$. Then there exists an irreducible factor $f_i(x)$ of $f(x)$ of degree > 1. Assume without loss of generality that $i = 1$. Consider $K = F[x]/(f_1(x))$. Because $f_1(x)$ is irreducible, K is a field. Furthermore, $F \subseteq K$. Let $r \in K$ be the image of x. Then r is a root of $f_1(x)$ in K, so $K \cong F(r)$. Therefore, over K, the polynomial $f_1(x)$ factors as

$$f_1(x) = (x - r)g_1(x).$$

Then

$$f(x) = (x - r)g_1(x)f_2(x) \cdots f_k(x)$$

over K. This implies that the number of irreducible factors of $f(x)$ over K is $> k$. By induction, $f(x)$ has a splitting field over K, call it E. Then

1. There exist $r_1, \ldots, r_n \in E$ such that $f(x) = (x - r_1) \cdots (x - r_n)$ over E.

2. $E = K(r_1, \ldots, r_n)$. We know that $f(r) = 0$, so without loss of generality say $r = r_1$. Then

$$E = K(r_1, \ldots, r_n) = F(r)(r_2, \ldots, r_n) = F(r_1, \ldots, r_n).$$

Thus E satisfies the two necessary conditions for a splitting field. □

9.3 example. Let $f(x) = x^2 + bx + c \in F[x]$.

If $f(x)$ factors over F, then F is a splitting field.

If $f(x)$ is irreducible over F, then $E = F[x]/(f(x))$ is a splitting field for $f(x)$, for the following reason. By construction, a root r_1 of $f(x)$ lies in E, so $f(x) = (x - r_1)g(x) \in E[x]$. By degree considerations, $g(x)$ is also linear, so both roots of $f(x)$ lie in E. Thus $E = F(r_1) = F(r_1, r_2)$ is a splitting field for $f(x)$.

9.4 example. Let $F = \mathbb{Q}$ and $f(x) = x^3 - 2 \in F[x]$. Then the roots of $f(x)$ in $\mathbb{C}$ are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$, where ω is a primitive 3rd root of unity. Let $K = \mathbb{Q}(\sqrt[3]{2}$. Then K is not a splitting field of $f(x)$ over $\mathbb{Q}$, because $\omega \notin K$, so $\omega\sqrt[3]{2} \notin K$. On the other hand, $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is a splitting for for $f(x)$ over $\mathbb{Q}$. The degree of this splitting field is $[\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}] = 6$.

Lecture 19
October 26th, 2017
Notes by Komal Agrawal

Now that we have discussed splittin fields of ploynomials, our next goal is to find an upper bound for $|Gal(E/F)|$

9.5 Lemma. *Consider an isomorphism $\varphi : F_1 \xrightarrow{\sim} F_2$. Then there exists a unique extension $\varphi : F_1[x] \to F_2[x]$ such that $\varphi(x) = x$. Hence, $\varphi(\sum_{i=0}^n a_i x^i) = \sum_{i=0}^n (\varphi(a_i))x^i)$*

9.6 Lemma. *Let $\varphi : F_1 \xrightarrow{\sim} F_2$ and supose $F_1 \subset E_1$ and $F_2 \subset E_2$. Let $r \in E_1$ be algebraic over F_1 with minimum polynomial $g(x)$. Then,*

1. *φ can be extended to an injection $F_1 \xhookrightarrow{\bar{\varphi}} E_2$ if and only if there exists $s \in E_2$ such that s is a root of $\varphi(g(x))$.*
2. *The number of such extensions $\bar{\varphi}$ equals the number of distinct roots of $\varphi(g(x))$ in E_2.*

Proof. As r is algebraic over F_1, we have $F_1(r) = F_1[r] = F_1[x]/g(x)$.

$$\begin{array}{ccc} F_1 & \xhookrightarrow{\varphi} & E_2 \\ \downarrow & \overset{\bar{\varphi}}{\nearrow} & \\ F_1[x] & & \end{array}$$

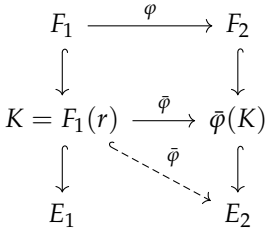
For any $s \in E_2$, $\exists!$ extension $F_1[x] \xrightarrow{\bar{\varphi}} E_2$ with $x \mapsto s$. Hence, by the universal properties of quotient, we have that an extension $\bar{\varphi} : F_1[r] \to E_2$ is precisely an

extension $\bar{\varphi} : F_1[x] \to E_2$ such that $\bar{\varphi}(g(x)) = 0$. We know that if $\bar{\varphi}(x) = s$, then $\bar{\varphi}(g(x)) = \bar{\varphi}(g)(s)$, that is, if $g(x) = \sum_{i=0}^{n} g_i x^i$ then $\bar{\varphi}(g(x)) = \sum_{i=0}^{n}(\varphi(g_i))s^i)$. So we get an extension $\bar{\varphi} : F_1(r) \to E_2$ iff $\bar{\varphi}(g)(s) = 0$ iff s is a root of $\varphi(g(x))$. □

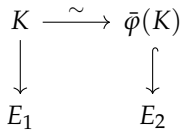
9.7 THEOREM. *Let $\varphi : F_1 \xrightarrow{\sim} F_2$ and $g(x) \in F_1[x]$ be monic of positive degree. Let E_1, E_2 be splitting fields of $g(x)$ and $\varphi(g(x))$ respectively over F_1 (and over F_2). Then,*

1. *There is an extension $\bar{\varphi} : E_1 \xrightarrow{\sim} E_2$ of the map φ.*
2. *The number of such extensions $\bar{\varphi}$ is $\leq [E_1 : F_1]$. If $\varphi(g(x))$ has distinct roots in E_2, then the number of extensions is exactly $[E_1 : F_1]$.*

Proof. We prove this by induction on $[E_1 : F_1]$.
Base Case: $[E_1 : F_1] = 1$.So. $E_1 = F_1$. Then $\exists r_1, \cdots, r_n$ such that $g(x) = \prod_{i=1}^{n}(x - r_i)$ in $F_1[X]$. $\varphi(g(x)) = \prod_{i=1}^{n}(x - \varphi(r_i))$ in F_2. So, $E_2 = F_2$ and $\bar{\varphi} = \varphi$ is the unique extension.
Induction Case: $[E_1 : F_1] = d > 0$. Factor $g(x)$ into irreducibles over $F_1[x]$ as $g(x) = g_1(x) \cdots g_a(x)$. Assume WLOG that $\deg(g_1(x)) > 1$.
In E_1, assume WLOG that $g_1(x) = \prod_{i=1}^{m}(x - r_i)$ and $(g(x)) = \prod_{i=1}^{n}(x - r_i)$.
In E_2, assume WLOG that $\varphi(g_1(x)) = \prod_{i=1}^{m}(x - s_i)$ and $\varphi(g(x)) = \prod_{i=1}^{n}(x - s_i)$.
Consider the following diagram



By lemma, $\exists$ an extension $\bar{\varphi} : F_1(r_1) \hookrightarrow E_2$ because $\varphi(g_1(x))$ has roots in E_2 and the number of such extensions is $\leq m$. Also, $[E_1 : F_1] = [E_1 : K][K : F_1]$ and as $[K : F_1] = m > 1$ so, $[E_1 : K] < d$. Now,



E_1 is a splitting field of $g(x)$ over K and E_2 is a splitting field of $\varphi(g(x))$ over $\bar{\varphi}(K)$. By induction, there exists an extension $\bar{\varphi} : E_1 \xrightarrow{\sim} E_2$ and the number of such extensions is $\leq [E_1 : K]$ and is exactly equal to $[E_1 : K]$ if $\bar{\varphi}(g(x))$ has distinct roots in E_2. For every distinct $\bar{\varphi} : F_1(r_1) \hookrightarrow E_2$, there are at most $[E_1 : K]$

extensions $E_1 \xrightarrow{\sim} E_2$. Hence, total number is $\leq m[E_1 : K] = d$. If $\varphi(g_1(x))$ has distinct roots in E_2 and $\varphi(g(x))$ has distinct roots in E_2, then the number of extensions $= d$. □

9.8 corollary. *Let $\varphi : F \to F$ be the identity map.*

1. *Let E_1, E_2 be splitting fields of some $f(x) \in F[x]$. Then, $E_1 \backsimeq E_2$.*
2. *If E is a splitting field of $f(x) \in F[x]$, then $|Gal(E/F)| \leq [E : F]$.*
3. *$|Gal(E/F)| = [E : F]$ if $f(x)$ has distinct roots in E.*

9.9 definition. Let F be a field and $f(x) \in F[x]$. If $f(x) = \sum_{i=0}^{n} a_i x^i$, the formal derivative is $f'(x) = \sum_{i=0}^{n} i a_i x^{i-1}$

Lecture 20
October 31st, 2017
Notes by Kenneth Allen

9.10 theorem. *If $f(x) \in F[X]$ is monic of positive degree, then all roots in any splitting field E/F are simple (i.e. are distinct) iff $gcd(f, f') = 1$.*

9.11 definition. $f(x) \in F[x]$ is called separable if $gcd(f, f') = 1$

9.12 definition. F is called perfect if every irreducible polynomial in $F[X]$ is separable.

If $charF = 0$ or F is finite, then F is perfect.

9.13 example. A classic example of a non-perfect field is $\mathbb{F}_p(t) = Frac(\mathbb{F}_p[t])$, over which $x^p - t$ is irreducible and non-separable.

Recall: If E/F, then $Gal(E/F) = \{\phi : E \to E | \phi(a) = a \forall a \in F\} \Rightarrow Gal(E/F) < Aut(E)$.

Recall: IF E is a splitting field of some $f(x) \in F[X]$, then $|Gal(E/F)| = [E : F]$ if $f(x)$ has distinct roots in E.

Let $f(x) = \prod f_i(x)^{e_i}$ where $f_i(x)$ are monic irreducible polynomials, $e_i \geq 1$. In fact, $|Gal(E/F)| = [E : F]$ if $\prod f_i(x)$ has distinct roots in E. This is true because the splitting field of $\prod f_i(x)$ is also E.

Remark: This is always true over perfect fields.

9.14 definition. Let E be any field. Let $G < AutE$ (any subgroup). The G-fixed field: $E^G = \{a \in E | \eta(a) = a \forall \eta \in G\}$

Claim: E^G is a field (Easy check).
$\{$Subgroups of $AutE\} \to \{$Subfields of $E\}$
$G \mapsto E^G$
$\{$Subfields of $E\} \to \{$Subgroups of $AutE\}$
$F \mapsto Gal(E/F)$

Broad question of Galois Theory: Can I expect these two maps to be related? Dream goal: mutually inverse bijection?

9.15 EXAMPLE. $f(x) = x^3 - 2$ over $\mathbb{Q} = F$

Consider $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ Not the splitting field, $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ is the splitting field where $\omega^3 = 3$, ω complex.

$Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{e\}$ trivial and $[\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}] = 3$.

9.16 PROPOSITION. *1) If $G_2 < G_1$, then $E^{G_1} \subset E^{G_2}$.*

2) If $F_2 \subset F_2$, then $Gal(E/F_1) < Gal(E/F_2)$.

3) $G < Gal(E/E^G)$

4) $F \subset E^{Gal(E/F)}$

Proof. 1) Let $G_2 < G_1$. Let $a \in E^{G_1}$, a is fixed by everything in G_1, so since $G_2 < G_1$, a is fixed by everything in G_2, so $E^{G_1} \subset E^{G_2}$.

2) Suppose $F_2 \subset F_1$. Let $\eta \in G$, η fixes F_1 pointwise, so it fixes F_2 pointwise. So $\eta \in Gal(E/F_2)$.

3) Let $\eta \in G$. We need η to fix E^G pointwise. However, $E^G =$ fixed set of G.

4) Exercise. □

9.17 LEMMA. *Artin. Let $G < Aut(E)$, finite subgroup. Let $F = E^G$. Then $[E : E^G] \leq |G|$.*

Proof. Let $n = |G|$. Take any m elements $u_1, \cdots, u_m \in E$, where $m > n$. We'll show that $\{a_i\}$ are F-linearly dependent. So, we want some $f_1, ..., f_m \in F$ (not all 0) so that $\sum f_i u_i = 0$. Let $G = \{\eta_1, ..., \eta_n\}$ and $\eta_1 = id$. Consider the matrix:

$$\begin{bmatrix} \eta_1(u_1) & \eta_1(u_2) & \dots & \eta_1(u_n) \\ \eta_2(u_1) & \eta_2(u_2) & \dots & \eta_2(u_n) \\ \vdots & \vdots & \vdots & \vdots \\ \eta_n(u_1) & \eta_n(u_2) & \dots & \eta_n(u_n) \end{bmatrix}$$

.

Consider the linear system:

$$\begin{bmatrix} \eta_1(u_1) & \eta_1(u_2) & \dots & \eta_1(u_m) \\ \eta_2(u_1) & \eta_2(u_2) & \dots & \eta_2(u_m) \\ \vdots & \vdots & \vdots & \vdots \\ \eta_n(u_1) & \eta_n(u_2) & \dots & \eta_n(u_m) \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

.

This system has a non-trivial solution over E. Choose a solution $(b_1, \cdots, b_m)$, where the number of non-zero b_i's is minimum. Claim: All of the b_i's in this solution actually lie in F. WLOG: Assume $b_1 \neq 0$. Assume that $b_1 = 1$ (by dividing by b_1). Look at first equation: $u_1 + b_2 u_2 + \cdots + b_m u_m = 0$, and for all

i, $\eta_i(u_1) + b_2\eta_i(u_2) + \cdots + b_m\eta_i(u_m) = 0$. Apply η_i^{-1}: $u_1 + \eta_i^{-1}(b_2)u_2 + \cdots + \eta_i^{-1}(b_m)u_m = 0$.

If not all $b_i \in F$, there exists some i which moves at least one of the b's. WLOG, suppose $\eta_i^{-1}(b_2) \neq b_2$. Take equation $(1) - (i)$: $(b_2 - \eta_i^{-1}(b_2))u_2 + (b_3 - \eta_i^{-1}(b_3)u_3 + \cdots = 0$. We can check that $(0, b_2 - \eta_i^{-1}(b_2), b_3 - \eta_i^{-1}(b_3), \cdots)$ is a new non-trivial solution of the system, contradicting the minimality of $(b_1, ..., b_m)$.

So: $[E : F] = [E : E^G] \leq G$. □

9.18 definition. Let E/F be an algebraic extension. 1) E/F is called normal if every irreducible $f(x) \in F[X]$ which has one root in E, has all roots in E. 2) E/F is called separable if the minimal polynomial of any $e \in E$ is separable over F. (Automatic for perfect fields).

9.19 example. $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is normal over $\mathbb{Q}$. $Gal(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ has size 6. $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ is the splitting field of $x^3 - 2$. One automorphism:

$$\begin{array}{cccccc} 1 & \alpha & \omega\alpha & \omega^2\alpha & \omega & \omega^2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & \omega\alpha & \omega^2\alpha & \alpha & \omega & \omega^2 \end{array}$$

Lecture 21
November 7th, 2017
Notes by Sergio E. Garcia Tapia and Joseph Dorta

9.2 *The Fundamental Theorem of Galois Theory*

Let E/F be Galis, and let $G = \text{Gal}(E/F)$. Also let Γ the set of all subgroups of G, and Σ be the set of all intermediate fields between E and F:

$$\Gamma = \{G\text{: G is a subgroup of } F\}, \quad \Sigma = \{F'\text{: } F' \text{is a field and } F \subset F' \subset F\}.$$

We have maps

$$\Gamma \to \Sigma, \quad \Sigma \to \Gamma,$$

such that

$$H \to E^H, \quad F' \to \text{Gal}(E/F').$$

Furthermore, given

1. These maps are mutually invertible bijections.
2. Given subgroups H_1, H_2 of G, $H_1 \supset H_2$ if and only if $E^{H_1} \subset E^{H_2}$.
3. $|H| = [E : E^H]$ and $[G : H] = [E^H : F]$ for each subgroup H of G.
4. $H \triangleleft G$ if and only if E^H is normal over F (which implies E^H/F is Galois).

Proof. 1. Consider $H \to E^H \to \text{Gal}(E/E^H)$. We know from before that $H \leq \text{Gal}(E/E^H)$, so that $|H| \leq \text{Gal}(E/E^H)$. Also, since the $\text{Gal}(E/E^H)$ is Galois, we have

$$|\text{Gal}(E/E^H)| = [E : E^H] \leq |H|,$$

by a Theorem from before. We conclude that $H = \text{Gal}(E/E^H)$. Furthermore, if $F' \in \Sigma$ and we consider

$$F' \to \text{Gal}(E/F') \to E^{\text{Gal}(E/F')}.$$

We wish to show that $F' = E^{\text{Gal}(E/F')}$. This is true because E/F' is Galois.

2. We proved this part in a previous Theorem.

3. The fact that $|H| = [E\colon E^H]$ was proved in the first part. The second equality follows from the this equality, since

$$[G\colon H] = \frac{|G|}{|H|} = \frac{[E : F]}{[E : E^H]} = [E^H : F],$$

by using the formula for the index of a group H in G and the formula for the degree of the extension for E over F.

4. Let $K = E^H$. Recall that $H \triangleleft G$ if and only if $\eta H \eta^{-1} = H$ for all $\eta \in G$. It is worth noting that, in general, the fixed of $\eta H \eta^{-1}$ is $\eta(K)$. This is because if $\eta(a) \in \eta(K)$ for some $a \in K$, then any element $\eta\xi\eta^{-1}$ of $\eta H \eta^{-1}$ fixes $\eta(a)$, precisely because $\xi(a) = a$. Therefore, $H \triangleleft G$ if and only if $\eta(K) = K$ for all $\eta \in G$ (though elements may not be fixed pointwise).

   ("$\Rightarrow$"): With this in mind, suppose that $\eta(K) = k$ for every $\eta \in G = \text{Gal}(E/F)$. We want to show that K/F is normal. Let $f(x) \in F[x]$ be irreducible, and let $\alpha \in K$ be a root of $f(x)$. Consider the set of Galois conjugates of α

$$S = \{\eta(\alpha) \mid \eta \in G\}.$$

   The set $S$is the orbit of α under G, and it is a subset of K because η fixes K. Put another way, the set S consists of all distinct roots of $f(x)$. Consider the polynomial

$$g(x) = \prod_{\beta \in S} (x - \beta).$$

   The coefficients of $g(x)$ are fixed by every element of G, as seen if applied η to $g(x)$, because the β are in K, and because the maps η are isomorphisms that permute β. Therefore, $g(x) \in F[x]$, since $F = E^G$, and we

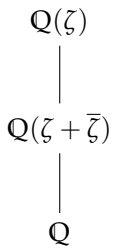


Figure 8: Subfield Lattice

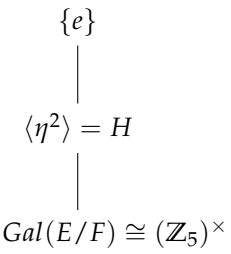


Figure 9: Subgroup Lattice

conclude that $g(x) \mid f(x)$ because it contains all of the roots of $f(x)$ as and its roots are simple. Since $f(x)$ is irreducible over F, we conclude that $f(x) = g(x)$, for $\deg(g(x)) \geq 1$. Consequently, if K has one of the roots of α, it has all of them, meaning that K/F is normal.

("$\Leftarrow$"): Now suppose that K/F is normal. We want to show that $\eta(K) = K$ for all $\eta \in G$, since this condition equivalent to H being a normal subgroup of G, as pointed out earlier. Let $\alpha \in K$, and let $f(x)$ be the minimum polynomial of α. Because η fixes $f(x)$ for every $\eta \in G$, $\eta(\alpha)$ must also be a root of $f(x)$. Also $f(x)$ is irreducible over F. By normality, $\eta(\alpha) \in K$, which implies that $\eta(K) \subset K$. Since η is an automorphism, it is bijective, so in fact $\eta(K) = K$, proving that $H \triangleleft G$.

□

9.20 example. 1. "Cyclotomic prime" examples: Let $p = 5$, then the polynomial $f(x) = \frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Q}$. Consider E, the splitting field of $f(x)$ over $\mathbb{Q}$. Then $E = \mathbb{Q}(\zeta)$, where $\zeta = e^{\frac{2\pi i}{5}}$, since the roots of $f(x)$ are $\zeta, \zeta^2, \zeta^3, \zeta^4$. The degree of this extension is thus $[E : F] = 5$, and the order of the Galois group is $|Gal(E/F)| = 4$. We deduce that the Galois group is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. We have the following subfield and subgroups lattices: Let $G = Gal(E/F)$. If $\eta \in G$, hence η is an automorphism fixing F and suppose $\eta(\zeta)$ is known,

then $\eta(\zeta)$ is also a root of $f(x)$, so $\eta(\zeta) = \zeta^i$ for some $1 \leq i \leq 4$. Note that η is entirely determined by this mapping since given any ζ^j we have $\eta(\zeta^i) = (\zeta^i)^j = \zeta^{ij}$ where we consider ij mod 5 since $\zeta^5 = 1$. We can then claim that $G \cong (\mathbb{Z}_5)^\times$ or equivalently $G \cong \mathbb{Z}_4$ via the map $\eta \mapsto i$ such that $\eta(\zeta) = \zeta^i$. Let's attempt to find a generator for G! Note that a generator for $(\mathbb{Z}_5)^\times$ is 2, hence$\eta : \zeta \mapsto \zeta^2$ is a generator for G, and as such we have $G = \langle 1 = id_E, \eta, \eta^2, \eta^3 \rangle$. Explicitly

- $\eta^2(\zeta) = \eta(\eta(\zeta)) = \eta(\zeta^2) = \zeta^4 = \overline{\zeta}$
- $\eta^3(\zeta) = \eta(\eta(\eta(\zeta))) = \eta(\eta(\zeta^2)) = \eta(\zeta^4) = \zeta^8 = \zeta^3$
- $\eta^4(\zeta) = \eta(\eta^3(\zeta)) = \eta(\zeta^3) = \zeta^6 = \zeta$

Note that $\eta^2(\zeta) = \overline{\zeta}$, so $\zeta + \overline{\zeta}$ is fixed under any element of the subgroup $H = \langle \eta^2 \rangle$. We claim that the corresponding fixed field is $[\mathbb{Q}(\zeta + \overline{\zeta}) : \mathbb{Q}]$ which has degree 2 over $\mathbb{Q}$.

2. Consider $f(x) = x^5 - 2$, and let $\alpha = 2^{\frac{1}{5}}, \zeta = e^{\frac{2\pi i}{5}}$, $E = \mathbb{Q}(\alpha, \zeta)$. Then we have the following subfield and subgroup lattices: We immediately

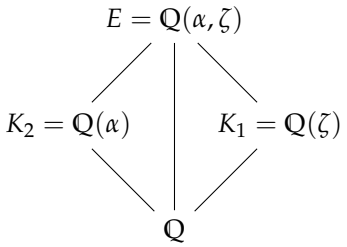


Figure 10: Subfield Lattice

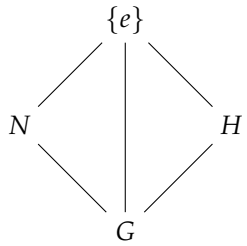


Figure 11: Subgroup Lattice

note, by the Galois correspondence that if$G := Gal(E/\mathbb{Q})$, then $|G| = 20 = [E/\mathbb{Q}]$. If we let $K_1 = \mathbb{Q}(\zeta)$,and $K_2 = \mathbb{Q}(\alpha)$ with corresponding subgroups H and N (resp.) of G, then we have $Gal(E/K_1) \cong \mathbb{Z}_5 \cong H$ and

$Gal(E/K_2) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ or$\mathbb{Z}_4$. Thus, we seek to determine N. We know K_1 is normal over $\mathbb{Q}$ and $Gal(K_1/\mathbb{Q}) \cong (\mathbb{Z}_5)^\times \cong G/N$. Noting that N is normal in G, we consider the short exact sequence:
$1 \to N \to G \to G/N \to 1$
By the correspondence above, we have $H = Gal(E/K_2), H \leq G, N \triangleleft G$. Note that since $|H| = 4, |N| = 5, H \cap N = e$, we have that $|HN| = 20 = |G|$ which implies that $G \cong N \rtimes_\phi H$, hence $G/N \cong H$. Thus we have the following more explicit splitting short exact sequence of groups:
$1 \to (\mathbb{Z}_5) \to G \to (\mathbb{Z}_5)^\times \to 1$
This leads us to the more explicit representations of N and H as follows:
$H = \langle \eta : \zeta \mapsto \zeta^2 \rangle, N = \langle \gamma : \alpha \mapsto \zeta\alpha \rangle$.

Part IV: Modules

10 Module Basics

Lecture 22
November 9th, 2017
Notes by Terrin Warren and Freddy Saia

Let A be an abelian group, then there exists a "$\mathbb{Z}$-action on A", a map

$$\mathbb{Z} \times A \to A$$
$$(n, a) \mapsto na.$$

If $n > 0$, then $na = \underbrace{a + a + \cdots + a}_{n \text{ times}}$.
If $n = 0$, then $na = 0$.
If $n < 0$, then $na = -(-n)a = \underbrace{-(a) + (-a) + \cdots + (-a)}_{-n \text{ times}}$

Under this map, the following properties hold for all $m, n \in \mathbb{Z}$, and $a, b \in A$:

1. $n(a + b) = na + nb$
2. $(m + n)a = ma + na$
3. $(mn)a = m(na)$
4. $1 \cdot a = a$

10.1 definition. Let R be a ring. A (left) R module is an abelian group with an action map

$$R \times M \to M$$
$$(r, n) \mapsto rn.$$

such that the following hold for $r, s \in R$ and $a, b \in M$:

1. $r(a + b) = ra + rb$
2. $(r + s)a = ra + sa$
3. $(rs)a = r(sa)$
4. $1_R \cdot a = a$

10.2 remark. This definition is true for any ring, whether it is commutative or not. In this course we will focus on the commutative case. Assume that all rings beyond this definition are commutative unless otherwise stated.

10.3 definition. Let M be an R module. A subgroup $N \leq M$ is an R submodule if for all $r \in R$, and all $n \in N$, $rn \in N$.

10.4 corollary. *Any $N \subset R$ is an R submodule if and only if N is an ideal in R.*

10.1 *Examples*

Now lets consider the following examples of modules.

1. $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{Z}$ are all $\mathbb{Z}$ modules. The action map is multiplication by n.

2. If R is any ring, then R is an R-module by the action

$$\begin{aligned} R \times R &\to R \\ (r, a) &\mapsto ra. \end{aligned}$$

3. If R is any ring, then for an ideal $I \subset R$, I is an R module by the action

$$\begin{aligned} R \times I &\to I \\ (r, i) &\mapsto ri. \end{aligned}$$

4. R/I is an R module by the action

$$\begin{aligned} R \times R/I &\to R/I \\ (r, s + I) &\mapsto rs + I. \end{aligned}$$

5. If K is any field and V is a K- vector space, then V is a K module by definition of a vector space.

6. If K is a field, then K is a $K[x]$ module in many different ways. One way is given by the map

$$\begin{aligned} K[x] \times K &\to K \\ (p(x), k) &\mapsto kp(d). \end{aligned}$$

   where d is any element in K.

7. Let K be any field and V a K- vector space and let $T : V \to V$ be a linear map. Then we have the following $K[x]$-module structure on V:

$$\begin{aligned} K[x] \times V &\to V \\ (p(x), v) &\mapsto p(T)v. \end{aligned}$$

   More concretely, suppose $V \cong \mathbb{R}^2$ with a basis e_1, e_2. Then let $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. and let $p(x) = x^2 - 1$.

Then $p(T) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 - \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$ and $p(T) \cdot e_1 = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0$ and $p(T) \cdot e_2 = \begin{pmatrix} 2 \\ 0 \end{pmatrix} = 2e_1$.

10.5 remark. If V is a K-vector space which has a $K[x]$-module structure, then there exists a linear map $T : V \to V$, such that $x \cdot v = T(v)$.

10.2 *Module homomorphisms and quotient modules*

Now that we have a new type of object, we proceed with some likely expected definitions:

10.6 definition. If M, N are two R-modules, then a group homomorphism $\phi : M \to N$ is an R-module homomorphism if $\phi(rm) = r\phi(m)$ for all $r \in R$ and all $m \in M$.

As usual, we define the kernal

$$\ker(\phi) = \{m \in M \mid \phi(m) = 0\}$$

and image

$$\mathrm{im}(\phi) = \{\phi(m) \mid m \in M\}$$

of ϕ. It can be checked that $\ker(\phi)$ and $\mathrm{im}(\phi)$ are R-submodules of M and N, respectively.

10.7 example. Let k be a field, then $k[x]$ is a $k[x]$-module in the way already described in the examples (i.e. the action is just multiplication in $k[x]$). With a choice of $d \in k$, we also saw that k is a $k[x]$ module with corresponding action

$$\begin{aligned} k[x] \times k &\to k \\ (f(x), a) &\mapsto f(d) \cdot a. \end{aligned}$$

Letting

$$\begin{aligned} \phi : k[x] &\to k \\ f(x) &\mapsto p(d), \end{aligned}$$

we claim that ϕ is a $k[x]$-module homomorphism. This is just the evaluation map at d, which we already know is a ring (and hence abelian group) homomorphism. Let $f(x), p(x) \in k[x]$, then

$$\begin{aligned} \phi(f(x)p(x)) &= f(d)(p(d)) \\ &= f(x) \cdot \phi(p(x)), \end{aligned}$$

where $\cdot$ here is denoting the chosen action of $k[x]$ on k as a $k[x]$-module. Our claim therefore holds.

In this example, we have

$$\begin{aligned}\ker(\phi) &= \{p(x) \in k[x] \mid p(d) = 0\} \\ &= (x-1).\end{aligned}$$

as an R-submodule of $k[x]$.

If M is an R-module with R-submodule N, then it can be checked that

$$M/N = \{m + N \mid m \in M\}$$

is also an R-module with corresponding action

$$(r, m+N) \mapsto rm + N.$$

Here, rm is simply the image of (r, m) under the action of R on M as an R-module. This map is well-defined because $rN \subset N$ for all $r \in R$ by definition of an R-submodule.

10.8 remark. We see that one of the nice properties of modules is that quotient modules can be obtained from arbitrary submodules. On the other hand, in the case of groups and rings, we needed special types of subgroups (normal subgroups) and special types of additive subgroups of rings (ideals) to construct quotient groups and rings. This property of modules is related to the category R-mod being an abelian category for a ring R. Another example of an abelian category is the category Ab of abelian groups, where in an analogous fashion quotients of a group can be constructed using arbitrary subgroups (as all subgroups are normal).

10.3 *Short exact sequences of modules*

Analogous to our definition for groups, a short exact sequence of R-modules for a ring R is a sequence

$$0 \longrightarrow M' \xrightarrow{\phi} M \xrightarrow{\phi} M'' \longrightarrow 0$$

of R-modules such that

(i) $\ker(\phi) = \{0\}$, i.e. ϕ is injective,

(ii) $\mathrm{im}(\psi) = M''$, i.e. ψ is surjective, and

(iii) $\ker(\psi) = \mathrm{im}(\phi)$.

In this case, by the first isomorphism for modules (proven in the same manner as that for groups) we get $M'' \cong M/\phi(M')$.

10.9 example. The sequence

$$0 \longrightarrow 2\mathbb{Z} \xhookrightarrow{\phi} \mathbb{Z} \xrightarrow{\psi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

where ϕ is the standard embedding of $2\mathbb{Z}$ into $\mathbb{Z}$ and ψ is the quotient projection map, is a short exact sequence of $\mathbb{Z}$-modules. Note that this sequence does not split (where a splitting is defined analogously to the case for groups) as there is no non-trivial injection of $\mathbb{Z}/2\mathbb{Z}$ into $\mathbb{Z}$.

10.4 *Direct sums of modules and their universal property*

Given two R-modules, we can define their direct sum (analogous to the direct product for groups and rings) as follows:

10.10 definition. If M_1, M_2 are R-modules, then it is not difficult to verify that

$$M_1 \oplus M_2 = \{(m_1, m_2) \mid m_1 \in M_1, m_2 \in M_3\}$$

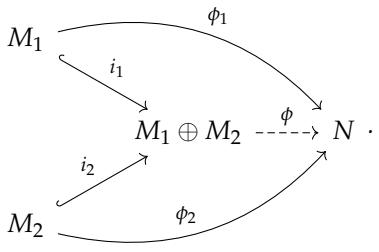
is also an R-module, where the corresponding R-action is simply obtained by the respective actions of R on each component.

It is clear that this definition may be extended to give the direct sum of any finite number of R-modules. Note that we get a standard embedding of M_1 into $M_1 \oplus M_2$:

$$i_1 : m_1 \mapsto (m_1, 0),$$

and similarly for M_2.

10.11 theorem (Universal property of the direct sum of modules). *If M_1, M_2, N are R-modules and $\phi_1 : M_1 \to N$ and $\phi_2 : M_2 \to N$ are R-module homomorphisms, then there exists a unique $\phi : M_1 \oplus M_2 \to N$ such that the following diagram commutes*



Proof. The proof for this theorem is analogous to that for the universal properties of direct products of other types of objects given previously, so we leave it as an exercise. □

Since R is itself an R-module for a ring R, for any $n \in \mathbb{N}$ we may consider

the direct sum of n copies of R:

$$R^{\oplus n} := \bigoplus_{i=1}^{n} R$$

which is again an R-module. This module has the special property that it has a basis: consider the set

$$\{e_i \mid i \in \{1, \dots, n\}\},$$

where $e_i \in R^{\oplus n}$ is the element

$$e_i = (0, \dots, 0, \underbrace{1}_{i^{\text{th}} \text{ position}}, 0, \dots, 0).$$

It is clear to see that this is a spanning set for $R^{\oplus n}$ as if $r = (r_1, \dots, r_n) \in R^{\oplus n}$ then

$$r = \sum_{i=1}^{n} r_i e_i.$$

Furthermore, we note that this set is R-linearly independent, as if

$$\sum_{i=1}^{n} s_i e_i = (0, \dots, 0)$$

for any $s_i \in R$, then s_i must be zero for all i. We call an R-module with a basis (i.e. an R-linearly independent spanning set) a free R-module.

11 Free modules

Lecture 23
November 14th, 2017
Notes by Jack Wagner and Nolan Schock

11.1 definition. Let M be an R-module. We say that $e_1, \dots, e_n$ form a basis for M if $e_1, \dots, e_n$ span M (i.e. any $m \in M$ can be expressed as an R-linear combination of $e_1, \dots, e_n$), and $e_1, \dots, e_n$ are linearly independent (i.e. if $\sum_{i=1}^{n} r_i e_i = 0$, then $r_i = 0$ for all i).

In the case of $R^{\oplus n}$, take $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ where 1 is in the i-th position, and elsewhere are all zeros. Then $e_1, \dots, e_n$ form a basis for $R^{\oplus n}$.

11.2 definition. An R-module is free of rank n if there exists elements $m_1, \dots, m_n \in M$ which form a basis for M.

A natural question is whether given a ring R, are all free R-modules are isomorphic to some $R^{\oplus n}$ for some n? The answer to this is yes.

11.3 CLAIM. *If M is a free module of rank n, then $M \cong R^{\oplus n}$.*

Proof. Let $\{e_1, \ldots, e_n\}$ be a basis for M. Define $f : M \to R^{\oplus n}$ where $e_i \mapsto (0, \ldots, 0, 1, 0, \ldots, 0)$ where the 1 is in the i-th position. First, we will check that f is an R-map. Notice that

$$\begin{aligned} f(s\sum_{i=1}^{n} r_i e_i) &= f(\sum_{i=1}^{n} s r_i e_i) \\ &= (sr_1, sr_2, \ldots, sr_n) \\ &= s(r_1, r_2, \ldots, r_n) \\ &= sf(\sum_{i=1}^{n} r_i e_i). \end{aligned}$$

It is clear that f is surjective and injective, thus f is an R-isomorphism. □

11.4 THEOREM. *Let M be an R-module.*

1. *If M is finitely generated, then any surjective morphism $M \to M$ is an isomorphism.*
2. *If $M \cong R^{\oplus n}$, then any set of n elements which spans M form a basis for M.*
3. *If M is free and is generated by n elements, then the rank of M is at most n.*
4. *If $m \neq n$, then $R^{\oplus m}$ and $R^{\oplus n}$ are not isomorphic.*

The proof of this theorem follows from linear algebra techniques, and will be shown later.

11.5 REMARK. In the first part, consider $f : \bigoplus_{i \in \mathbb{N}} R \to \bigoplus_{i \in \mathbb{N}} R$ where $f(e_{2r-1}) = e_r$ and $f(e_{2r}) = e_r$. Notice that $\bigoplus_{i \in \mathbb{N}} R$ is not finitely generated, but f is surjective. Notice too that $f(e_1) = f(e_2) = e_1$, so f is not an isomorphism.

The next question to consider is whether the submodules of a free R-module are free.

11.6 EXAMPLE. Consider R as a free R-module of rank 1. Suppose R is a PID. Any submodule of R is an ideal of R. That means that if N is a submodule, then $N \cong (d)$ for some $d \in R$. Therefore, N is free of rank 1.

11.7 EXAMPLE. Let $R = \mathbb{C}[x, y]$, which is not a PID. Let $I = (x, y)$, which is not principle.

11.8 CLAIM. *Regarding I as a submodule of R, I is not free.*

Proof. Suppose I is free. I is not a principle ideal, therefore I has to be generated by at least 2 elements. This implies that $I \cong R^{\oplus n}$ for some $n \geq 2$. Let f be

an isomorphism $I \to R^{\oplus n}$. Consider $f(x)$ and $f(y)$, which spans $R^{\oplus n}$. By the theorem, we get that $f(x)$ and $f(y)$ form a basis. However,

$$\begin{aligned} yf(x) - xf(y) &= f(yx) - f(xy) \\ &= f(yx - xy) \\ &= f(0) = 0, \end{aligned}$$

so $f(x)$ and $f(y)$ are not linearly independent. This contradicts that they form a basis. □

11.9 theorem. *If R is a PID and M is a free R-module of rank n, then any submodule of M is free of rank at most n.*

11.10 remark. We will prove the above theorem by induction on the rank of R. Note that we have already proven the rank 1 case.

11.11 Lemma. *Let M be an R-module. Suppose there is a surjective map $\varphi : M \to R^{\oplus n}$. Then there is some R-module N such that there is an isomorphism $\psi : M \to R^{\oplus n} \oplus N$, and if $\pi : R^{\oplus n} \oplus N \to R^{\oplus n}$ is the natural projection map, then $\varphi = \pi \circ \psi$, as in the following diagram.*

$$\begin{array}{ccc} M & \xrightarrow{\psi} & R^{\oplus n} \oplus N \\ & \searrow^{\varphi} & \downarrow \pi \\ & & R^{\oplus n} \end{array}$$

Proof. Let $N = \ker \varphi$. Let $e_1, \ldots, e_n$ be a basis for $R^{\oplus n}$. Because φ is surjective, there exist $m_1, \ldots, m_n \in M$ such that $\varphi(m_i) = e_i$. Define $\eta : R^{\oplus n} \to M$ by $\eta(e_i) = m_i$. Then $\varphi(\eta(e_i)) = \varphi(m_i) = e_i$, hence $\varphi \circ \eta = id_{R^{\oplus n}}$. This implies that η is injective. Now define $\psi : M \to R^{\oplus n} \oplus N$ by $\psi(m) = (\varphi(m), m - \eta(\varphi(m))$. Note that $m - \eta(\varphi(m)) \in N = \ker \varphi$, since

$$\varphi(m - \eta(\varphi(m)) = \varphi(m) - \varphi(\eta(\varphi(m))) = \varphi(m) - \varphi(m) = 0,$$

hence ψ is well-defined.

Now, note that

$$\begin{aligned} \psi(m_1 + m_2) &= (\varphi(m_1 + m_2), m_1 + m_2 - \eta(\varphi(m_1 + m_2))) \\ &= (\varphi(m_1) + \varphi(m_2), m_1 - \eta(\varphi(m_1)) + m_2 - \eta(\varphi(m_2))) \\ &= \psi(m_1) + \psi(m_2), \end{aligned}$$

and

$$\begin{aligned}\psi(rm) &= (\varphi(rm), rm - \eta(\varphi(rm))) \\ &= (r\varphi(m), r(m - \eta(\varphi(m))) \\ &= r\psi(m),\end{aligned}$$

hence ψ is an R-module homomorphism.

Now suppose $m \in \ker\psi$. Then $\psi(m) = (\varphi(m), m - \eta(\varphi(m))) = 0$. This implies that $\varphi(m) = m - \eta(\varphi(m)) = 0$. Thus $m \in \ker\varphi$, so $m - \eta(\varphi(m)) = m - \eta(0) = 0$, hence $\eta(0) = m$. But η is injective, so $m = 0$. Thus ψ is injective.

Finally, let $(p, q) \in R^{\oplus n} \oplus N$. Let $m = \eta(p) + q$. Then

$$\psi(m) = (\varphi(\eta(p)) + \varphi(q), \eta(p) + q - \eta(\varphi(m))) = (p, q),$$

hence ψ is surjective.

We conclude that ψ is an isomorphism as desired. □

Proof of Theorem. As mentioned previously, we use induction on the rank of M, and the base case has already been proven.

Suppose the result holds for $n \geq 1$. Let M be a submodule of $R^{\oplus n+1}$. Let $\pi : R^{\oplus n+1} \to R^{\oplus n}$ be the natural projection, leaving the last n coordinates. Now let $N = \pi(M) \subseteq R^{\oplus n}$. By induction, $N \cong R^{\oplus m}$ for some $m \leq n$. We have the following composition of maps.

$$M \xrightarrow{\ i\ } R^{\oplus n+1} \xrightarrow{\ \pi\ } R^{\oplus n},$$

with i the natural inclusion map, and N a submodule of $R^{\oplus n}$. Then the image of $\pi \circ i$ is in fact equal to N, so $\pi \circ i$ is surjective. By the lemma, we can thus write $M \cong N \oplus \ker\pi|_M$.

Finally, observe that $\ker\pi|_M \cong M \cap R \subseteq R$. Thus $M \cap R \cong R$ is free, so $M \cong N \oplus \ker\pi|_M \cong N \oplus R$ is free. □

Lecture 24
November 16th, 2017
Notes by Kenneth Allen and

11.12 THEOREM. *R is a PID, then any submodule of a free module of rank n is free of rank $\leq n$.*

11.13 EXAMPLE. $R = \mathbb{Z}$, $M = \{(a, a, b) \in \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}\} \subset \mathbb{Z}^{\oplus 3} = \mathbb{Z}^3$.

$M \xrightarrow{\pi} \mathbb{Z}^2$

$(a, a, b) \mapsto (a, b)$

$M \cong \mathbb{Z}^2 \oplus Ker\pi$

$Ker\pi = \{(a, a, b) | a = 0 \text{ and } b = 0\} = \{(0, 0, 0)\}$

So $M \cong \mathbb{Z}^2$

So $rk(M) = 2$

A free basis of M is then given by $\pi^{-1}(e_1), \pi^{-1}(e_2)$ under the map π.

$e_1 = \begin{bmatrix}1\\0\end{bmatrix}, e_2 = \begin{bmatrix}0\\1\end{bmatrix}$

$\pi^{-1}(e_1) = \begin{bmatrix}1\\1\\0\end{bmatrix}, \pi^{-1}(e_2) = \begin{bmatrix}0\\0\\1\end{bmatrix}$ free basis for M.

Different basis $\{\begin{bmatrix}1\\1\\2\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}\} = \{m_1 + 2m_2, m_2\}$

$\begin{bmatrix}1 & 0\\2 & 1\end{bmatrix}$ is the change of basis matrix, which is invertible over $\mathbb{Z}$.

Set up: $M' \subset M$, where M and M' are free R modules, R is a PID.

More generally: $M' \xrightarrow{A} M$: A is a module map between free modules M' and M.

11.14 example. $M' = \mathbb{Z}$, $M = \mathbb{Z}^2$

$M' \hookrightarrow M$

$a \mapsto (a, 0)$

$\{1\}$ and $\{e_1, e_2\}$ are bases.

$1 \mapsto e_1$

11.15 example. $M' = \mathbb{Z}$, $M = \mathbb{Z}^2$

$M' \hookrightarrow M$

$a \mapsto (a, a)$

$1 \mapsto e_1 + e_2$ (not just a multiple of a basis vector).

11.16 definition. Let $M' \hookrightarrow M$ free R-modules. Let $\{b_1, b_2, \cdots, b_n\}$ be a basis of M. We say that M' has a basis aligned with $\{b_1, b_2, \cdots, b_n\}$ if there exists $d_1, \cdots, d_k \in R$ such that $\{d_1 b_1, d_2 b_2, \cdots, d_k b_k\}$ is a basis of M'.

11.17 definition. Let $A : M' \to M$ be a map of free R-modules. Let $\{b_1, b_2, \cdots, b_n\}$ be a basis of M and $\{b'_1, b'_2, \cdots, b'_m\}$ be a basis of M'. We say these bases are aligned if there are non-zero $d_1, \cdots, d_k \in R$ such that $A(b'_i) = \begin{cases} d_i b_i & i \leq k \\ 0 & \text{otherwise} \end{cases}$

Equivalently, the matrix of A in these bases is: $\begin{bmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_k & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix}$

(Not necessarily square).

11.18 EXAMPLE. $\mathbb{Z} \xrightarrow{i_1} \mathbb{Z} \oplus \mathbb{Z}$, $1 \mapsto \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

Matrix of i_1 is $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$, bases are aligned.

11.19 EXAMPLE. $\mathbb{Z} \xrightarrow{\Delta} \mathbb{Z} \oplus \mathbb{Z}$, $1 \mapsto \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

Matrix of Δ is $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$, bases are not aligned.

11.20 THEOREM. *Let M', M be free R-modules and let $A : M' \to M$ be a module map. 1) Then there exists bases $\{b_1, b_2, \cdots, b_n\}$ and $\{b'_1, b'_2, \cdots, b'_m\}$ of M and M' respectively such that they are aligned with respect to A. 2) In fact we can change basis so that*

$$A = \begin{bmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_k & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix}$$

And where $d_i | d_{i+1}$ for all i.

11.21 EXAMPLE. $\mathbb{Z} \xrightarrow{\Delta} \mathbb{Z} \oplus \mathbb{Z}$. $\{e_1, e_2\}$ is not aligned. Change basis of $\mathbb{Z} \oplus \mathbb{Z}$ to $\{\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}\}$. Then the matrix of Δ in this basis is $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $d_1 = 1$.

11.22 EXAMPLE. $\mathbb{Z} \oplus \mathbb{Z} \xrightarrow{A} \mathbb{Z} \oplus \mathbb{Z}$, $(m, n) \mapsto (2m, 3n)$. Matrix of A is $\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$

Exercise: It is possible to change bases so that the new matrix is $\begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}$.

Idea to prove theorem: Apply suitable row and column operations tio the matrix of A to bring A to the desired form. Given the matrix of A, we are allowed to make it PAQ, where $P \in GL_n(R), Q \in GL_m(R)$.