Lecture Notes Math 371: Algebra (Fall 2006)

by Nathanael Leedom Ackerman

September 14, 2006

0.1 TALK SLOWLY AND WRITE NEATLY!!

0.2 Abelian Group

0.2.1 Definitions

Definition of Abelian Group

Definition 0.2.1.1. We say a group $\langle A, +, 0 >$ is Abelian if

$$(\forall a, b \in A) a + b = b + a$$

Spanning Notation

Definition 0.2.1.2. Let G be a group and let $g_1, g_2, \cdots \in G$. We then define $\langle g_1, g_2, \cdots \rangle$ = subgroup of G generated by $g_1, g_2, \cdots$

Torsion Subgroup

Definition 0.2.1.3. Let $\langle G, +, 0 \rangle$ be an abelian group and let $a \in G$. We say a is a torsion element if it has finite order.

The collection of all torsion elements of an Abelian group A is called the Torsion Subgroup of A

A group A is said to be of exponent m if every element of A has period dividing m.

Lemma 0.2.1.4. *If A is abelian then the torsion subgroup of A is a subgroup of A*

Proof. Notice that if $na = 0$ then $na^{-1} = 0$ and if $na = 0$ and $mb = 0$ then $nm(a + b) = 0$. □

Free Group

Definition 0.2.1.5. We say an abelian group A is free if

- $A = Span\langle u_1, \cdots, u_r \rangle$
- $\Sigma_{i \leq r} a_i u_i = 0 \Rightarrow a_i = 0$ for all $i \leq r$

We then say A has rank r.

0.2.2 Theorems

Subgroups of Free Groups are Free

Theorem 0.2.2.1 (Dedekind)**.** *Let F be a free abelian group of rank r and let G be a subgroup of F. Then G is a free abelian group of rank $s \leq r$. Further F has a set of generators $\langle u_i, \cdots, u_r \rangle$ such that G is generated by*

$$\begin{array}{rcccccccc} v_1 & = & a_{11}u_1 & + & a_{12}u_2 & + & \ldots & + & a_{1r}u_r \\ v_2 & = & & + & a_{12}u_2 & + & \ldots & + & a_{2r}u_r \\ \vdots & & & & \vdots & & & & \vdots \\ v_s & = & & & a_{ss}u_s & + & \ldots & + & a_{sr}u_r \end{array}$$

for some a_{ij} such that all a_{ii} which are positive.

Proof. Let $\langle u_i, \cdots, u_r \rangle$ be a basis for F for notational convenience we will say that $x = \Sigma_{i \leq r} c(x, i)u_i$ for all $x \in$.

Now choose some non-zero element $b = \Sigma_{i \leq r} c(b, i)u_i$ of

G.

By reordering the indexes and possibly taking inverses of some of the basis elements we can assume that $c(b,1) > 0$.

Now lets look at all the values of $c(b,1)$ for $b \in G$ and choose a minimum positive value (which we know must exist because $c(b,1) > 0$). Call the smallest such integer a_{11} and pick some element v such that $c(v,1) = a_{11}$

We therefore have that if $x = \Sigma_{i \leq r} c(x,i)u_i \in G$ then a_{11} divides $c(x,1)$. This is because $c(x,1) = p * a_{11} + a$ where $a < a_{11}$. And so if a_{11} didn't divide $c(x,1)$ then $-pv_1 + x$ would have a coordinate in u_1 with coefficient less than a_{11}.

So in particular, for all $x \in G$ there is a q such that $x - qv_1 = c(x,2)u_2 + \cdots + c(x,r)u_r$.

If $r = 1$ we are done.

Assume $r > 1$ but the theorem is true for all $r - 1$. The theorem breaks into two cases.

Case 1: $G \subseteq Span(u_2, \cdots, u_n)$

Then we are done by induction.

Case 2: $\neg G \subseteq Span(u_2, \cdots, u_n)$

Then let $F_1 = Span\langle u_2, \cdots, u_r\rangle$ and $G_1 = G \cap F_1$. This theorem then applies to F_1, G_1 as $G_1 \subseteq F_1$ and so we have that $G_1 = Span\langle v_2, \cdots, v_s\rangle$ with $s \leq r$ and

further

$$\begin{array}{rcccccccc} v_2 & = & a_{22}u_2 & + & a_{23}u_3 & + & \dots & + & a_{2r}u_r \\ v_3 & = & & + & a_{33}u_3 & + & \dots & + & a_{3r}u_r \\ \vdots & & & & \vdots & & & & \vdots \\ v_s & = & & & a_{ss}u_s & + & \dots & + & a_{sr}u_r \end{array}$$

with $a_{22} \cdots a_{ss}$ all positive.

Hence we know that $G = Span\langle v_1, \cdots, v_s \rangle$ by the inductive hypothesis.

So all that is left is to check that $v_1, \cdots, v_n$ are independent. If not then there are some $\Sigma_{i \leq r} d_i v_i = 0$ where $d_i \in \mathbb{Z}$

But we know that if $r = 1$ this can't happen. And hence by induction we that $\langle v_s, \cdots, v_r \rangle$ are independent. So this means that there must be some linear combination of v_i which adds to 0 and what is more this must have

the coeffecient of v_1 non-zero.

$$-d_1v_1 = d_2v_2 + \cdots + d_nv_n$$

But, putting any such linear combination in terms of the u_i we see that $d_1 = 0$ (as v_1 is the only element with u_1 component and the u_i's are linearly independent). $\Rightarrow\Leftarrow$.

Hence the $\langle v_1, \cdots, v_s \rangle$ are a linear independent basis for F as a free abelian group. □

Theorem about basis

Theorem 0.2.2.2. *Let $F = \langle u_1, \cdots, u_r \rangle$ and let $v = b_1u_1 + \cdots + b_ru_r$ with $gcd(b_1, \cdots, b_r) = 1$. Then there exists $v_2, \ldots v_r \in F$ such that $F = \langle v, v_2, \ldots, v_r \rangle$.*

Proof. Set $s = |b_1| + |b_2| + \cdots + |b_r|$. If $s = 1$ then the result is trivial as $v = \pm u_i$ for some i.

Now lets assume this theorem is true for all $0 \leq r < s$.

As $s > 1$ we know that at least 2 of the b_i's are non-zero. With out loss of generality we can assume $b_1 \geq b_2 > 0$ (although we may have to change the signs of some of the basis elements)

Now lets let $w_1 = u_1, w_2 = u_1 + u_2, w_j = u_j$ if $j \geq 3$. We then clearly have $F = \langle w_1, \ldots, w_r \rangle$ and also that $v = (b_1 - b_2)w_1 + b_2 w_2 + \cdots + b_r w_r$.

Further, $gcd(b_1 - b_2, b_2, \ldots, b_r) = 1$ and

$$|b_1 - b_2| + |b_2| + \ldots |b_r| < s$$

And so the result follows by induction. □

Relation of Basis of Free Group to Subgroup

Theorem 0.2.2.3. *Let F be a finitely generated free abelian group of rank r and let G be a subgroup of F of*

rank s with $0 < s \leq r$. Then there exists $v_1, \ldots, v_r \in F$ such that

$$F = \langle v_1, \ldots, v_r \rangle$$

$$G = \langle h_1 v_1, \ldots, h_r v_r \rangle$$

where $h_1, \ldots, h_r$ are all positive and satisfy h_i divides h_{i+1}.

Proof. Let $u_1, \ldots, u_r$ be a set of generators for F. Take $x \in G$ and write $x = x_1 u_1 + \cdots + x_r u_r$. We then define $\delta^{\langle u_1, \ldots, u_r \rangle}(x) = gcd(x_1, \cdots, x_r)$.

Lemma 0.2.2.4. *$\delta^{\langle u_1, \ldots, u_r \rangle}(x)$ is independent of the choice of generators.*

Proof. We know by the definition of x that

$$x = \delta^{\langle u_1, \ldots, u_r \rangle}(x)(y_1 u_1 + \cdots + y_r u_r)$$

for some integers r.

Now let $w_1, \cdots, w_r$ generate F. Then we can represent each u_i in terms of $w_1, \cdots, w_r$. Hence

$$x = \delta^{\langle u_1,\ldots,u_r\rangle}(x)(y_1^* w_1 + \cdots + y_r^* w_r)$$

and so $\delta^{\langle u_1,\ldots,u_r\rangle}(x)$ divides $\delta^{\langle w_1,\ldots,w_r\rangle}(x)$.

And so by symmetry we must have $\delta^{\langle u_1,\ldots,u_r\rangle}(x) = \delta^{\langle w_1,\ldots,w_r\rangle}(x)$

□

We will then simply write $\delta(x)$ for $\delta^{\langle u_1,\ldots,u_r\rangle}(x)$.

Now take any nonzero $y_1 \in G$ such that $\delta(y_1)$ is minimal. Set $h_1 = \delta(y_1)$. We then have

$$y_1 = h_1(z_1 u_1 + \cdots + z_r u_r)$$

where $gcd(z_1, \cdots, z_r) = 1$. So in particular by the previous lemma we know that if we set $v_1 = z_1 u_1 + \cdots + z_r u_r$ then there exist $v_2^*, \cdots, v_r^*$ such that

$$\langle v_1, v_2^*, \ldots, v_r^* \rangle = F$$

If $r = 1$ then we are done because we have $s = 1$, $F = \langle v_1 \rangle, G = \langle h_1 v_1 \rangle$.

So lets do induction on r. Suppose $r > 1$.

Let $F_1 = \langle v_2^*, \ldots, v_r^* \rangle$ and let $G_1 = F_1 \cap G$. Then G_1 is a subgroup of F_1. There are two cases we must consider.

Case 1: $\text{Rank}(G_1) = 0$.

In this case we know that $G_1 = 0$ and so $G = \langle h v_1 \rangle$

Case 2: $\text{Rank}(G_1) > 0$.

In this case we know by the inductive hypothesis that there are $\langle v_2, \ldots, v_r \rangle$ such that

$$F_1 = \langle v_2, \ldots, v_r \rangle$$

$$G_1 = \langle h_2 v_2, \ldots, h_r v_r \rangle$$

and h_i divides h_{i+1}.

But we therefore know that

$$F = \langle v_1, v_2, \ldots, v_r \rangle$$

Now lets consider a $y \in G$. Well then we know we can write

$$y = a_1 v_1 + a_2 v_2^* + \cdots + a_r v_r^*$$

But we know $a_1 = qh_1 + m$ for some $m < h_1$ and further $\delta(y - qy_1) \leq m$. Hence $m = 0$ because we choose y_1 to be such that $\delta(y)$ was minimal. So h_1 divides a_1.

So we have $y - qh_1 v_1 = t_2 v_2^* + \cdots + t_r v_r^*$

Hence

$$G_1 = \langle h_1 v_1, h_2 v_2, \ldots, h_r v_r \rangle$$

and all that is left to show is that h_1 divides h_2.

let $h_2 = ah_1 + b$ where $0 \leq b < h_1$. Then if we let $\alpha = h_1 v_1 + h_2 v_2 \in G$ we have $\gcd(y_0) = gcd(h_1, h_2) = gcd(h_1, b)$. Hence by the minimality of h_1 we have $b = 0$.

So by induction we are done. □

0.3 The Structure Theorem for Finitely Generated Abelian Groups

0.3.1 Theorem

From the previous theorem we have

Existence of Decomposition By Increasing Div

Theorem 0.3.1.1. *Every finitely generated Abelian group A can be expressed as the direct sum of cyclic groups*

$$A \cong \mathbb{Z}^m \oplus \mathbb{Z}/h_1 \oplus \cdots \oplus \mathbb{Z}/h_j$$

where h_i divides h_{i+1}

Proof. Let A be a finitely generated Abelian group such that

$$A = \langle u_1, \ldots, u_n \rangle$$

Now consider the map $\varphi : \mathbb{Z}^n \to A$ where $\varphi(e_i) = u_i$ (and e_i is the ith basis element).

This map is obviously surjective and so we know that

$$A \cong \mathbb{Z}^n / ker(\varphi)$$

But $ker(\varphi)$ is a subgroup of $\mathbb{Z}^n$ and hence there is a basis $\langle f_1, \ldots, f_n \rangle$ for $\mathbb{Z}^n$ such that

$$ker(\varphi) = \langle h_1 f_1, \ldots, h_r f_r \rangle$$

and h_i divides h_{i+1}. Hence

$$A \cong (\langle f_1 \rangle / \langle h_1 f_1 \rangle) \oplus \cdots \oplus (\langle f_r \rangle / \langle h_r f_r \rangle) \oplus \cdots \oplus (\langle f_n \rangle)$$

hence

$$A \cong \mathbb{Z}^m \oplus \mathbb{Z}/h_1 \oplus \cdots \oplus \mathbb{Z}/h_j$$

and we are done. □

But what is more, is that this decomposition is unique. Specifically we have

Uniqueness of Decomposition By Increasing D

Theorem 0.3.1.2. *Let A be a finitely generated Abelian group. Let*

$$A = \mathbb{Z}^r \oplus \mathbb{Z}/e_1 \oplus \cdots \oplus \mathbb{Z}/h_n$$

where e_i divides e_{i+1} and

$$A = \mathbb{Z}^s \oplus \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_m$$

where d_i divides d_{i+1}. Then $s = r$, $m = n$ and $e_i = d_i$ for all i

But before we show this we need another theorem.

Existence of Decomposition By Sylow Subgrou

Theorem 0.3.1.3. *Let G be a finite abelian group of order $p_1^{a_1}p_2^{a_2}\cdots$ where the p_i's are distinct primes. Then*

$$G = P_1 \oplus P_2 \oplus \cdots$$

Where P_i are the subgroups of elements of G with order a power of p_i.

Proof. Let $x \in G$ be an element of order $p_1^{\alpha} f_1$ where p_1 and f_1 are relatively prime. We can then find u, v such that $uf_1 + vp_1^{\alpha} = 1$.

We then have $x = uf_1x + vp_1^{\alpha}x$ but we know that uf_1x has order p_1^{α} and $vp_1^{\alpha}x$ has order f_1.

So we know we can break $x = b_1 + x_1$ where b_1 has order p_1^{α} and x_1 has order f_1. And so by iterating this process we can break $x = b_1 + b_2 + \ldots$ where b_i has order $p_i^{a_i}$

So, if we can show that this decomposition is unique we are done.

Suppose we have $b_1 + b_2 + \cdots = x = b_1^* + b_2^* + \ldots$ where b_i, b_i^* has order p_i^α.

We then have that there are $c_1 + c_2 + \cdots = 0$ where each c_i has order a power of p_i.

But this means that $-c_i = c_1 + \ldots c_{i-1} + \ldots c_{i+1} + \ldots$.
And so $p_1^{a_1} \ldots p_{i-1}^{a_{i-1}} \ldots p_{i+1}^{a_{i+1}} \ldots (c_i) = 0$. But this is only true if $c_i = 0$.

Hence $c_i = b_i - b_i^* = 0$ and so $b_i = b_i^*$ for all i

And so we are done. □

Decomposition of Cyclic Group Into Sylow Su

Corollary 0.3.1.4. *Let* $e = p_1^{a_1} \cdots p_m^{a_m}$. *Then*

$$\mathbb{Z}/(e) \cong \mathbb{Z}/(p_1^{a_1}) \oplus \cdots \oplus \mathbb{Z}/(p_m^{a_m})$$

Proof. We know

$$\mathbb{Z}/(e) = P_1 \oplus P_2 \oplus \cdots$$

where $P_i = \{z \in \mathbb{Z}/(e) : \text{order}(z) \text{ is a power of } p_i\}$.
In particular if x generates $\mathbb{Z}/(e)$ then we have

$$x = q_1 \oplus \cdots \oplus q_n$$

where each q_i has order a power of p_i.

but every $y \in \mathbb{Z}/(e) = mx$ and so in particular this means that every $z \in \mathbb{Z}/(e)$ of order $p_i = m_z x$.

So in particular $(n/p_i^{a_i})z = (n/p_i^{a_i})m_z x = (n/p_i^{a_i})m_z q_i$.

But as $n/p_i^{a_i}$ is relatively prime to $p_i^{a_i}$ there is an integer s such that $s * n/p_i^{a_i} \equiv 1 \bmod p_i^{a_i}$.

So $s(n/p_i^{a_i})z = z = (n/p_i^{a_i})m_z q_i = m_z q_i$ (because order of $(n/p_i^{a_i})z = p_i^{a_i}$).

In particular this means that P_i is generated by a single element and hence $P_i \cong \mathbb{Z}/(p_i^{a_i})$ and we have

$$\mathbb{Z}/(e) \cong \mathbb{Z}/(p_1^{a1}) \oplus \cdots \oplus \mathbb{Z}/(p_m^{a_m})$$

□

Now we can return to the proof of the uniqueness of the decomposition.

Proof Uniqueness of Decomposition By Increas

Proof. First to see that $r = s$ notice that

$$A \cong \mathbb{Z}^s \oplus T \cong \mathbb{Z}^r \oplus T$$

where T is the torsion group of A.

So if $\pi_r : A \to \mathbb{Z}^r$ then

$$im(\pi_r) = \mathbb{Z}_r \cong A/ker(\phi_r) = A/T$$

But similarly if $\pi_s : A \to \mathbb{Z}^s$ then

$$im(\pi_s) = \mathbb{Z}_s \cong A/ker(\phi_s) = A/T$$

So we must have $\mathbb{Z}_s \cong \mathbb{Z}_r$ and hence $r = s$.

Now lets just look at the torsion group T.

First we need a lemma

Lemma 0.3.1.5. *Let G be any group. Suppose $x, y \in G$ and $xy = yx$ and the order of x is relatively prime to the order of y. Then*

$$\langle x, y >= \langle xy \rangle$$

and is cyclic of (order(x))(order(y)).

Proof. Let order$(x) = n$ and order$(y) = m$.

First observe that $\langle xy \rangle \subseteq \langle x, y \rangle$

But then we also have $(xy)^m = x^m$. However, because m, n are coprime there is a α such that $\alpha \cdot m \equiv 1 (mod n)$. And so $(xy)^{(\alpha+1)m} = x$. And we can get y in an identical manner and so we see

$$\langle x, y \rangle = \langle xy \rangle$$

Now we know the order of $\langle x, y \rangle \leq mn$ as every element is of the form $x^a y^b$ with $0 \leq a \leq n-1, 0 \leq b \leq m-1$.

Suppose we have $(xy)^t = 1$. Then we know that $(xy)^{mt} = x^{mt}$ and so n divides mt. But as m, n are coprime this means that n divides t. We similarly get that n divides t and so t is divisible by mn. Hence the order of $\langle xy \rangle$ is

at least mn.

But we have already shown that it is at most mn and hence the order must be exactly mn. □

For clarity lets let $e_i = p_1(i)^{a_1(i)} \cdots p_w(i)^{a_w(i)}$. We therefor know that $a_j(i) \leq a_j(k)$ or all $i \leq k$ (by our assumption on the e_i).

But we also know that

$$(1)T = \oplus_{i \leq m}(\oplus_{j \leq w}\mathbb{Z}/(p_j(i)^{a_j(i)}))$$

So in particular we have

$$T = \oplus_{j \leq w}(\oplus_{i \leq m}\mathbb{Z}/(p_j(i)^{a_j(i)}))$$

Hence we have that if H is any p_j-Sylow subgroup of T

$$H \cong \oplus_{i \leq m}\mathbb{Z}/(p_j(i)^{a_j(i)})$$

Further if we have a decomposition of the form $(*)$ then this implies that it must have come (uniquely) from the

decomposition

$$T = \mathbb{Z}/(e_1) \oplus \mathbb{Z}/(e_m)$$

(by the nature of the e_i's)

So, in order to prove the theorem, all that is left is to prove that the decomposition of the p_j-Sylow groups is unique.

Decomposition of Abelian p-Groups

Theorem 0.3.1.6. *Let A be an abelian group of order p^a where p is prime. Suppose*

$$A \cong \langle u_1 \rangle \oplus \cdots \oplus \langle u_k \rangle$$

and

$$A \cong \langle v_1 \rangle \oplus \cdots \oplus \langle v_l \rangle$$

where order$(u_i) = f_i$, order$(v_j) = g_j$,

$$f_1 \geq f_2 \geq \cdots \geq f_k > 1$$

and

$$g_1 \geq g_2 \geq \cdots \geq g_l > 1$$

Then $k = l$ *and* $f_i = g_i$ *for all* i.

Proof. The first thing to notice is that

$$f_1 + f_2 + \cdots + f_k = a = g_1 + g_2 + \cdots g_l$$

Now we will prove the theorem by induction.

Base Case: If $a = 1$ this result is trivial as $f_1 = g_1 = a$.

Inductive Case: Assume this is true for $a < \alpha$ and now assume $a = \alpha$.

Let $A_p = \{x \in A : px = 0\}$. So we have

$$A_p = \langle p^{f_1-1}u_1\rangle \oplus \cdots \oplus \langle p^{f_k-1}u_k\rangle$$

$$A_p = \langle p^{g_1-1}v_1\rangle \oplus \cdots \oplus \langle p^{g_l-1}v_l\rangle$$

Hence $A_p = [\mathbb{Z}/(p)]^l = [\mathbb{Z}/(p)]^k$ and so $l = k$.

Now lets consider $A^p = \{px : x \in A\}$. Now if γ is such that $g_\gamma > 1$ but $g_{\gamma+1} = 1$ and κ is such that $f_\kappa > 1$ but $f_{\kappa+1} = 1$ then we have

$$A^p = \langle pu_1\rangle \oplus \cdots \oplus \langle pu_\kappa\rangle$$

$$A^p = \langle pv_1\rangle \oplus \cdots \oplus \langle pv_\gamma\rangle$$

But then by the inductive hypothesis we have $\kappa = \gamma$ and $f_i - 1 = g_i - 1$ for all $i \leq \kappa$.

And so we are done with this theorem $\square$

And this also proves the main theorem. □

0.4 Modules

0.4.1 Definition

ONLY IF TIME

0.5 TODO

- Specifically figure out what to show other than the structure theorem.
- Come up with A BUNCH of examples (more than I can use) so that I don't run out of time.