Instructor: Miklos Abert
Scribe: Aaron Marcus
July 10, 2006.

7. Lecture 7

7.1. **An interesting finite group.** Let p be a prime number, and consider a height two tree such that all non-leaf nodes of the tree have p children. Fixing a cyclic permutation σ of p elements, we can consider G, the subgroup of the automorphism group of the tree where the children of each node are permuted by some power of σ. Since there are $p+1$ parent nodes, and since each node can be independently permuted p ways, $|G| = p^{p+1}$.

What is $Z(G)$ the center of G? If $g \in G$, then the only way $gh = hg\ \forall h \in G$ is for g to fix the height 1 nodes and to act identically on each of their children. Thus $|Z(G) = p|$. Let $x \in G$. If x leaves the height 1 nodes fixed, then $x^p = 1$. If x does not leave the height 1 nodes fixed, and acts as σ^{c_i} on the children of the ith height 1 node, then x^p leaves the height 1 nodes fixed and acts as $\sigma^{\Sigma c_i}$ on each of their children. Therefore, $x^p \in Z(G)$.

Putting this information together, we see that $|G/Z(G)| = p^p$ and if $x \in G/Z(G)$, then $x^p = 1$. Thus, there are large p-groups with every element of order p.

7.2. **Some group theory.** Recall that a group G is residually finite if for every $x \in G \setminus \{1o$, there is some normal subgroup N_x, such that $x \notin N_x$ and G/N_x is a finite group. Moreover, if N_x can always be chosen such that G/N_x is a p-group, G is a residual p-group.

Theorem 7.1. *Every finitely generated linear group is residually finite.*

Theorem 7.2. *Every finitely generated linear group in characteristic 0 (e.g. over a base field $\mathbb{R}$ or $\mathbb{C}$) has a finite index subgroup with no elements of finite order.*

Corollary 7.3. *A finitely generated periodic linear group in characteristic 0 is finite.*

Proof. The only subgroup of a periodic group with no elements of positive finite order is 1, and since there must be such a subgroup with finite index, the group must be finite. □

To prove these theorems, we need some results from commutative algebra.

7.3. **Some commutative algebra.** In this section, F will be some fixed field, and R is a finitely generated subring of F. That is to say that every element of R can be written as a polynomial of some set of generators $\{k_1, \dots, k_n\}$. Equivalently, R is the image of the substitution map $\mathbb{Z}[x_1, \dots, x_n] \to F$.

Definition 7.4. The index of an ideal $I \subset R$ is the number of elements in R/I. Alternately, it is the index of I in R viewed as a subgroup of R under addition.

Theorem 7.5. *Every maximal ideal $\mathfrak{m} \subset R$ has finite index.*

Definition 7.6. Given a ring, S, the Jacobson radical $J(S)$ is the intersection of all maximal ideals of S.

Theorem 7.7. *With R as above, $J(R) = 0$.*

Given two ideals, $I, J \subset R$, we define their product $IJ = \langle ab | a \in I, b \in J \rangle$, the ideal containing all finite linear combinations of products from I and J. Note that $IJ \subset I \cap J$. In general, equality does not hold.

Theorem 7.8. *With R as above, if $I \subset R$ is a proper ideal, then $\cap_n I^n = 0$.*

Theorem 7.9. *If* $\mathrm{char}(\mathrm{F}) = 0$*, then* $pR = R$ *for only finitely many primes* $p \in \mathbb{Z}$*.*

Let $GL_n(R)$ be the group of all invertible $n \times n$ matrices with entries in R. If $\Gamma \subset GL_n(F)$ is finitely generated, say $\Gamma =< g_1, \ldots, g_k >$, then let R be the subring of F generated by the $2kn^2$ entries of g_i, g_i^{-1}. Then R is a finitely generated subring of F and $\Gamma \subset GL_n(R)$.

Let $I \subset R$ be an ideal, and let $\Gamma(I) = \Gamma \cap (1 + M_n(I))$. Then $\Gamma(I) \triangleleft \Gamma$ and if I has finite index in R, then $\Gamma(I)$ has finite index in Γ.

Let $\mathfrak{m} \subset R$ be a maximal ideal. By theorem 7.5, $R/\mathfrak{m}$ is a finite field, F_q, where $q = p^\alpha$, p prime, $\alpha \in \mathbb{N}$. Since $R/\mathfrak{m}$ is a field of characteristic p, we must have that $p \in \mathfrak{m}$. Therefore, for all $n \in \mathbb{N}$, $p\mathfrak{m}^n \subset \mathfrak{m}^{n+1}$ and so $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is an additive group of exponent p.

Let $x \in \Gamma(\mathfrak{m}^n)$. Then $x \equiv 1 \pmod{\mathfrak{m}^n}$, so $p(x-1) \equiv 0 \pmod{\mathfrak{m}^{n+1}}$ and $(x-1)^p \equiv 0 \pmod{\mathfrak{m}^{n+1}}$. Therefore, if $x \equiv 1 \pmod{\mathfrak{m}^n}$, then $x^p \equiv ((x-1)+1)^p \equiv 1 \pmod{\mathfrak{m}^{n+1}}$, so $\Gamma(\mathfrak{m}^n)/\Gamma(\mathfrak{m}^{n+1})$ is a p-group. Inductively, $\Gamma/\Gamma(\mathfrak{m}^n)$ is a p-group.

If $\Gamma \subset GL_n(\mathbb{C})$ is finitely generated, then $\Gamma \subset GL_n(R)$ for some finitely generated subring R. For all but finitely many primes $p \in \mathbb{Z}$, $pR \neq R$, and so $pR \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. $R/\mathfrak{m}$ is a finite field with $p \equiv 0$, and so must be of characteristic p. Let $x \in \Gamma$. Then since $\cap \mathfrak{m}^n = 0$, if $x \in \Gamma, x \neq 1$, there is some n such that $x \notin \Gamma(\mathfrak{m}^n)$. Therefore, we have the following theorem.

Theorem 7.10. *If* $\Gamma \subset GL_n(\mathbb{C})$ *is a finitely generated subgroup, then for all but finitely many primes* p*, there exists a finite index subgroup* $H \subset \Gamma$ *such that* H *is a residual* p*-group.*

Let p_1, p_2 be two such primes, and let H_1, H_2 be corresponding subgroups. Let $H = H_1 \cap H_2$. H is of finite index, and every finite cyclic subgroup of H is of exponent p_1 and p_2, and thus H is trivial. Therefore, Γ is finite.