Wielandt's Theorem on Automorphism Towers

Notes by Richard Foote

I have always wondered whether Wielandt's Theorem on the finiteness of automorphism towers could be made more transparent by couching a proof in the more modern terminology of components, etc. (One classic book containing a proof is [**Zas**], Appendix G.) Here is my attempt. I make no claim that this proof is better, shorter or even significantly different from either the original or proofs in various books; but rather this is a record of my musings on the subject. I am also especially grateful to Dr. Hy Ginsberg for his careful reading and stimulating comments on these notes.

Notation is standard, as may be found in [**DF**] or [**Asc**]. All groups in this note are finite. Throughout the notes, "acts" means "acts by conjugation." For completeness, the cited exercises from [**DF**] are included in the Appendix at the end of Section C. Section D, added later, is an interesting, self-contained example.

Recall that a group G acts on itself by conjugation resulting in a homomorphism

$$G \longrightarrow \mathrm{Aut}(G)$$

whose kernel is the center of G (see [**DF**], Section 4.4 and its exercises for definitions and basic facts). In particular, if $Z(G)=1$, then this is an embedding, and we may identify G with its group of inner automorphisms, which, by Exercise 4.4.1, forms a normal subgroup of $\mathrm{Aut}(G)$. It is immediate too from this exercise that if G has trivial center, then the center of $\mathrm{Aut}(G)$ is likewise trivial, so we may repeat the process. Replacing the homomorphisms, as above, by containments, we then iteratively obtain a tower:

$$\begin{gathered}\textit{If } Z(G)=1 \textit{ we have}\\ G=A_0 \trianglelefteq A_1 \trianglelefteq A_2 \trianglelefteq \cdots \trianglelefteq A_n = A \qquad \textit{where} \qquad A_{i+1}=\mathrm{Aut}(A_i), \quad 0 \le i \le n-1.\end{gathered} \tag{$*$}$$

Wielandt's beautiful result asserts that this automorphism tower eventually stabilizes:

Theorem (*H. Wielandt, 1939)* Under the hypotheses of $(*)$, there is some N such that $A_i = A_N$ for all $i \ge N$. (Equivalently, in any such tower, the order of A_n is bounded by some function of $|G|$, independent of n.)

Note that the order of the automorphism group of any centerless group X is bounded by $|X|!$ because $\mathrm{Aut}(X)$ faithfully permutes the elements of X. Therefore, to prove Wielandt's Theorem it suffices to find certain (finitely many) specific subgroups X_i of G such that $|A_n|$ is bounded in terms of $|\mathrm{Aut}(X_i)|$. At the heart of this process lies the *generalized Fitting subgroup* of G, and its fundamental property, due to Helmut Bender. For convenience we review this subject area.

B. Background Preliminaries

Let p be a prime and let X, H be groups. The results in this section, labeled **B.i** for integers **i**, might be considered as part of the "bread-and-butter" toolkit for finite group theorists! Experts may skip this section.

Recall that H is a *subnormal subgroup* of X if there is a chain

$$H = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = X \tag{$**$}$$

where each H_i is normal in H_{i+1} (but not necessarily normal in X). This is usually denoted by $H \trianglelefteq\trianglelefteq X$. For example, by [**DF**] Section 6.1, every subgroup of a nilpotent group is subnormal (and conversely). Note that "subnormality" is transitive. Also, such H is subnormal in every subgroup of X containing it.

A subgroup L of X is called a *component* of X if the following hold:

(i) $L \trianglelefteq\trianglelefteq X$,

(ii) L is perfect, i.e., $L = [L, L]$, and

(iii) $L/Z(L)$ is a (non-abelian) simple group.

A group satisfying only (ii) and (iii) is called *quasisimple*; so a component of X is a quasisimple subnormal subgroup of X. Non-abelian simple groups are, a fortiori, quasisimple. $SL_2(\mathbb{F}_5)$ is a quasisimple group of order 120 with a center of order 2.

Define $E(X)$ *to be the group generated by all components of* X*.*

B.1 $E(X) = L_1 * L_2 * \cdots * L_r$ is a (commuting) central product of all the components L_i of X.
(*Proof:* See [**Asc**], 31.7.)

B.2 The only normal subgroups of $E(X)$ are products of some of the L_i together with some subgroup of the center of $E(X)$.
(*Proof:* Ibid. This follows also from [**DF**], Exercise 5.4.18 applied to $E(X)/Z(E(X))$.)

B.3 The *Fitting subgroup* of X, denoted by $F(X)$, is the largest normal nilpotent subgroup of X. Also,

$$F(X) = O_{p_1}(X) \times O_{p_2}(X) \times \cdots \times O_{p_s}(X)$$

where $p_1, \ldots, p_s$ are all the distinct primes dividing $|X|$.
(*Proof:* Easy exercise. See [**Asc**], 31.8.)

B.4 $E(X)$ and $F(X)$ commute and are both characteristic in X.
(*Proof:* This follows from B.2 and B.3; see also [**Asc**], 31.12.)

Define the *generalized Fitting subgroup* of X, denoted by $F^*(X)$, to be $F^*(X) := F(X)E(X)$.

B.5 *(The Generalized Fitting Subgroup Theorem)* $C_X(F^*(X)) = Z(F^*(X))$.
(*Proof:* See [**Asc**], 31.13. Note that $F^*(X)$ is characteristic in X.)

B.6 As a direct consequence of B.5 and the opening remarks of this note we get:

$$\textit{For any finite group } X, \qquad |X| \leq |Z(F^*(X))| \cdot |\mathrm{Aut}(F^*(X))|.$$

In particular, if $M = |F^*(X)|$, then an upper bound for $|X|$ is $M \cdot M!$. This is crude because, in particular, automorphisms of a group cannot be arbitrary permutations of that group: they must all fix the identity, preserve the orders of elements, etc.

B.7 *(Three Subgroups Lemma)* Let H, E be any subgroups of X with E perfect. If $[H, E, E] = 1$, then $[H, E] = 1$.
(*Proof:* See [**Asc**], 8.9. Strictly speaking this is just a consequence of the more generally formulated Three Subgroups Lemma in [**Asc**].)

Recall that $O^p(X)$ is the *smallest* normal subgroup of X for which $X/O^p(X)$ is a p-group. It is easy to see that $O^p(X)$ is the subgroup generated by all elements of X of order prime to p.

B.8 If $H \trianglelefteq\trianglelefteq X$ and $|X : H|$ is a power of p, then $O^p(X) = O^p(H)$.
(*Proof:* This is an easy induction on m in $(**)$.)

C. Proof of Wielandt's Theorem

Henceforth let G be a finite group with $Z(G) = 1$. Adopt the notation of $(*)$. By the Generalized Fitting Subgroup Theorem (or, more precisely, B.6) it suffices to bound $|F^*(A)|$ in terms of $|G|$. We do this by bounding $|E(A)|$ and then $|F(A)|$ separately, in a series of steps.

Step 1: $C_A(G) = 1$.

Proof: Proceed by induction on the length, n, of the chain in $(*)$. If $n = 0$ then $G = A$ and $C_G(G) = Z(G) = 1$. If $n = 1$ then the result is the observation that $A_1 = \mathrm{Aut}(G)$ acts faithfully on G, made earlier. For $n \geq 2$, by induction we have $C_{A_{n-1}}(G) = 1$. Let $C = C_A(G)$. Then since $G \trianglelefteq A_1$, we see that A_1 normalizes C; and since $A_1 \leq A_{n-1} \trianglelefteq A$ we have

$$[C, A_1] \leq C \cap A_{n-1} = C_{A_{n-1}}(G) = 1,$$

i.e., $C \leq C_A(A_1)$. By definition of C the reverse containment is obvious, so $C = C_A(A_1)$. Now again use induction with G replaced by A_1, so that the chain starting at A_1 has length $n-1$, to get $C = 1$.

Step 2: $E(A) = E(G)$.

Proof: By induction on n we have $E(A_{n-1}) = E(G)$. Since $E(G)$ is subnormal in A, each component of $E(G)$ is likewise a component of A, hence is a component of $E(A)$. Let E_2 be the central product of all components of A that are *not* contained in G (so not in A_{n-1} too), hence by B.1:

$$E(A) = E(G) * E_2$$

where $*$ denotes central product; and both factors are normalized by G. Since $G \leq A_{n-1} \trianglelefteq A$ we have

$$[G, E_2] \leq E_2 \cap A_{n-1}.$$

Since the right-hand side intersection above is normal in E_2, by definition of E_2 and B.2 we have $[G, E_2] \leq Z(E_2)$. Thus $[G, E_2, E_2] = 1$. Since E_2 is perfect, by B.7 we have $[G, E_2] = 1$, i.e., $E_2 \leq C_A(G)$. The result now follows from Step 1.

Step 2 accomplishes the first stage of our proof of Wielandt. We next bound $|F(A)|$ in terms of $|G|$. It suffices to bound the number of distinct primes p dividing $|F(A)|$ and each $|O_p(A)|$.

Step 3: For every prime p, $O_p(A)$ normalizes and acts faithfully by conjugation on $O^p(G)$. Moreover, if p does not divide $|G|$ then $O_p(A) = 1$.

Proof: For an arbitrary prime p let $X = O_p(A)G$, and let P be a Sylow p-subgroup of X. By B.8,

$$O^p(G) = O^p(X) \trianglelefteq X, \tag{3.1}$$

as needed for the normality assertion. Note too that $X = PO^p(G)$. Let $P_0 = C_P(O^p(G)) \trianglelefteq P$. Since $P_0 \trianglelefteq P$, if $P_0 \neq 1$ then $P_1 := P_0 \cap Z(P) \neq 1$. Thus P_1 centralizes both P and $O^p(G)$, which generate X. Hence $P_1 \leq C_X(G)$, which is trivial by Step 1; and so $P_0 = 1$ as well. Since $O_p(A) \leq O_p(X) \leq P$, this proves the second assertion of Step 3. Moreover, if p does not divide $|G|$, then $O^p(G) = G$ and so by (3.1) we have $[O_p(A), G] \leq O_p(A) \cap G = 1$, i.e., $O_p(A) \leq C_X(G) = 1$, as needed to finish the proof of Step 3.

Wielandt's Theorem now follows easily: By Step 3, for all primes p not dividing $|G|$ we have $O_p(A) = 1$, and we also have

$$|F(A)| \leq \prod_{p \mid |G|} |\mathrm{Aut}(O^p(G))|.$$

Combining this with Step 2 gives

$$|F^*(A)| \leq |E(G)| \cdot \prod_{p \mid |G|} |\mathrm{Aut}(O^p(G))|.$$

So $|A_n|$ is (crudely) bounded above, independent of n in $(*)$, by B.6 applied to the above. (In fact, $|F^*(A)|$ *divides* the above product, even when we replace each factor of $|\mathrm{Aut}(O^p(G))|$ by just its p-part.)

Exercises

Let G be a finite group with $Z(G) = 1$. Adopt the notation of $(*)$.

1. Prove that $N_A(G) = A_1$. Deduce that if $G \trianglelefteq A$ then $A_2 = A_1$, i.e., the tower terminates in at most one step.

2. Let G be a direct product of non-abelian simple groups. Prove that $A_2 = A_1$ in $(*)$.

3. What hypotheses do you need on an arbitrary tower $(*)$—where each $A_i \trianglelefteq A_{i+1}$ but A_{i+1} need *not* equal $\mathrm{Aut}(A_i)$—to obtain the bound on $F^*(A)$ at the end of the proof? [Note that Steps 2 and 3 only rely on Step 1 of the proof.]

References

[Asc] *Finite Group Theory*, M. Aschbacher, Cambridge U. Press, 1986.

[DF] *Abstract Algebra, third edition*, D. Dummit and R. Foote, Wiley, 2003.

[Zas] *The Theory of Groups*, H. Zassenhaus, Chelsea, 1958.

Appendix — Cited exercises from [DF]

4.1.1. If $\sigma \in \mathrm{Aut}(G)$ and ϕ_g is (left) conjugation by g prove that $\sigma\phi_g\sigma^{-1} = \phi_{\sigma(g)}$. Deduce that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. (The group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the *outer automorphism group* of G.)

5.4.18. Let $K_1, K_2, \ldots, K_n$ be non-abelian simple groups and let $G = K_1 \times K_2 \times \cdots \times K_n$. Prove that every normal subgroup of G is of the form G_I for some subset I of $\{1, 2, \ldots, n\}$ (where G_I is the direct product of the K_i for $i \in I$).
[Hint: If $N \trianglelefteq G$ and $x = (a_1, \ldots, a_n) \in N$ with some $a_i \neq 1$, then show that there is some $g_i \in G_i$ not commuting with a_i. Show $[(1, \ldots, g_i, \ldots, 1), x] \in K_i \cap N$ and deduce $K_i \leq N$.]

D. Example of Towers of Arbitrary Length

This discussion creates strictly increasing automorphism towers of arbitrary length (for different starting groups G). The fundamental idea is that if $K := \langle\, r, s \,\rangle$ is a dihedral group of order 2^{N+1} for $N \geq 2$ with usual generators r, s of orders $2^N, 2$ respectively, and if $K_i := \langle\, r^{2^N - i}, s \,\rangle$, then K_i is a dihedral subgroup of order 2^{i+1} and

$$K_2 \trianglelefteq K_3 \trianglelefteq \cdots \trianglelefteq K_N = K \qquad \text{with} \qquad K_{i+1} = N_K(K_i).$$

(We shall prove this momentarily.) This alone is not quite good enough to produce an automorphism tower because both $Z(K_i) \neq 1$ and generally $K_{i+1} \neq \mathrm{Aut}(K_i)$—the latter is a much bigger group (see the exercises following). So we need some additional "constraints" to mitigate these shortcomings. We do this essentially by letting K act on a 2-dimensional vector space over $\mathbb{F}_p$ for a suitable prime p. The details follow.

First let 2^n be given, for any fixed $n \geq 2$. We assert that there is some prime p such that 2^n divides $p-1$ as follows (sketch): Let p be a prime dividing $2^{2^{n-1}} + 1$, so $2^{2^{n-1}} \equiv -1 \pmod{p}$. One easily argues that the multiplicative order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$ is 2^n. Then use Lagrange to verify that $2^n \mid p-1$. *For the remainder of the discussion let p be a prime chosen with $p - 1 = 2^N d$ where d is odd and $N \geq 4$.* (Think of N as being large!)

Next we generalize and provide more detail for the opening paragraph. Let $K = D_{2^{N+1}d} = \langle\, r, s \,\rangle$ be the dihedral group of order $2^{N+1}d$, where d is odd, with the usual generators r, s of orders $2^N d$ and 2 respectively. Let $R_i = \langle\, r^{2^{N-i}} \,\rangle$ be the unique subgroup of $\langle\, r \,\rangle$ of order $2^i d$ for $1 \leq i \leq N$, and let $K_i = \langle\, R_i, s \,\rangle$ be the dihedral subgroup of K or order $2^{i+1}d$ containing s. We sketch that

$$K_i \text{ is a subgroup of index 2 in } K_{i+1} \text{ and } N_K(K_i) = K_{i+1}. \tag{1}$$

It is easy that $K_i \leq K_{i+1}$ and $|K_{i+1} : K_i| = 2$ so $K_i \trianglelefteq K_{i+1}$. To show K_{i+1} is the full normalizer of K_i in K, first compute that $[r^m, s] = r^{-2m}$. This implies that $[R_m, s] = R_{m-1}$ for every $m \geq 2$. Let $N = N_K(K_i)$, so $K_{i+1} \leq N$. To prove the reverse containment observe that $N \cap \langle\, r \,\rangle$ is a cyclic subgroup of index 2 in N containing R_{i+1}, hence it must equal R_m, for some $m \geq i+1$. Since $s \in K_i$ we have $[R_m, s] = R_{m-1} \leq K_i$, hence $m - 1 \leq i$, as needed for the reverse containment, and so (1) holds.

[Note that, up to conjugacy in K, there are two choices for the generator s, namely a given s and then rs. The proof in the preceding paragraph works regardless of which conjugate we choose; and this is reflected by the fact that s and rs are conjugate under the outer automorphism of K of order 2, given by the action of $D_{2^{N+2}d}$ containing K as a (normal) subgroup of index 2.]

Next let $V = E_{p^2}$ be the the elementary abelian group of order p^2 for p as above. Note that $\mathrm{Aut}(V) = GL_2(\mathbb{F}_p)$, which has order $p(p-1)^2(p+1)$. It is helpful to notice that because $4 \mid p - 1$ and $(p-1, p+1) = 2$, we get $4 \nmid p+1$, so a Sylow 2-subgroup of $GL_2(\mathbb{F}_p)$ has order 2^{2N+1}. We shall write $GL_2(\mathbb{F}_p)$ as a 2×2 matrix group with identity I. Let $\mathbb{F}_p^\times = \langle \zeta \rangle$, so ζ is a primitive $(p-1)^{\mathrm{st}}$ root of unity in $\mathbb{F}_p$. Define the following elements of $GL_2(\mathbb{F}_p)$:

$$z = \zeta I = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta \end{pmatrix} \qquad r = \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix} \qquad s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

so $|r| = p - 1 = |z|$; also, $s^2 = 1$ and $r^s = srs = \begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix}$. Let $Z = \langle\, z \,\rangle \cong Z_{p-1}$ (this is the center of $GL_2(\mathbb{F}_p)$). Thus $\langle\, r, r^s \,\rangle$ is homocyclic abelian of order $(p-1)^2$ and

$$\langle\, r, s \,\rangle \cong (Z_{p-1} \times Z_{p-1}) \cdot Z_2 \cong Z_{p-1} \wr Z_2.$$

Note that $Z \leq \langle r, s \rangle$, and $\langle r, s \rangle$ is the largest subgroup of $GL_2(\mathbb{F}_p)$ that permutes the two eigenspaces of r acting on V spanned by $(1,0)$ and $(0,1)$. [We could further argue that $\langle r, s \rangle$ is a maximal subgroup of $GL_2(\mathbb{F}_p)$.]

Next we define certain subgroups of $\langle r, s \rangle$. For each $0 \leq i \leq N$ let

$$r_i := r^{2^{N-i}}, \qquad \text{so } |r_i| = 2^i d.$$

Now let

(a) $W_i := \langle r_i, s \rangle \cong Z_{2^i d} \wr Z_2$

(b) $C_i := \langle r_i r_i^s \rangle = Z \cap W_i \cong Z_{2^i d}$

(c) $L_i := \langle W_i, Z \rangle \cong (Z_{2^i d} \wr Z_2) * Z_{p-1}$ where the two factors in this central product intersect in the cyclic group C_i.

Next note that

$$(\zeta^{-(2^N-i)} I) \cdot r_i^s = \begin{pmatrix} \zeta^{-(2^N-i)} & 0 \\ 0 & \zeta^{-(2^N-i)} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \zeta^{2^{N-i}} \end{pmatrix} = r_i^{-1}.$$

In other words, conjugation by s inverts $r_i \pmod{Z}$. Since $\langle r_i \rangle \cap Z = 1$, the order of $r_i \pmod{Z}$ in L_i/Z is the same as $|r_i|$, hence we have

(d) $L_i/Z \cong D_{2\cdot(2^i d)}$.

It follows that

(e) $L_2 \trianglelefteq L_3 \trianglelefteq \cdots \trianglelefteq L_N$ with each $|L_{i+1} : L_i| = 2$,

where, since Z is contained in every L_i, one can verify this computation by working (mod Z) and just comparing successive orders.

We also easily have:

(f) $L_i' = W_i' = \langle [r_i, s] \rangle = \langle r_i^{-1} r_i^s \rangle \cong Z_{2^i d}$, for $i \geq 2$.

We also need a couple of facts about the projective linear groups $PGL_2(\mathbb{F}_p) := GL_2(\mathbb{F}_p)/Z$ and $PSL_2(\mathbb{F}_p) := SL_2(\mathbb{F}_p)Z/Z$. Proofs are relegated to the exercises at the end of this section.

(g) $|PGL_2(\mathbb{F}_p) : PSL_2(\mathbb{F}_p)| = 2$. Also, $PSL_2(\mathbb{F}_p)$ has one class of involutions (it is sufficient that conjugation takes place in $GL_2(\mathbb{F}_p)$), and the centralizer in $PGL_2(\mathbb{F}_p)$ of a (projective) involution in $PSL_2(\mathbb{F}_p)$ is isomorphic to L_N/Z.

The key "taming" construction is as follows. Let X be the semidirect product $V \rtimes GL_2(\mathbb{F}_p)$, where the action of $GL_2(\mathbb{F}_p)$ on V is the natural one. For each $i \geq 2$ let $A_i := V \rtimes L_i \leq X$. Note that A_i is a normal subgroup of index 2 in A_{i+1}. Also observe that the non-abelian group L_i acts faithfully and (consequently also) irreducibly on V, so it follows easily that

$$Z(A_i) = 1, \qquad 2 \leq i \leq N.$$

We finish the main proof by arguing that as abstract groups,

$$A_{i+1} \cong \mathrm{Aut}(A_i), \qquad 2 \leq i \leq N-1. \tag{2}$$

Fix $i \geq 2$, let $B := \mathrm{Aut}(A_i)$, and identify A_i as a normal subgroup of B as before. Note that $V = O_p(A_i)$ is characteristic in A_i, so under this identification $V \trianglelefteq B$. Since A_{i+1} acts faithfully by conjugation on A_i, we have $A_{i+1} \leq B$.

We first claim

$$B \text{ acts on } V \text{ with the kernel of this action equal to } V, \text{ for all } i \geq 2. \tag{3}$$

To see this, let $C = C_B(V)$. Thus C centralizes V and commutes with the faithful action of L_i on V; so C also acts trivially on A_i/V. Hence C stabilizes the chain $1 \leq V \leq A_i$, i.e., acts trivially on the two successive quotients. (See Corollary 32 and its following paragraph in Section 17.3 of [**DF**] for relevant definitions and results on stability groups.) By Corollary 17.2.29 in [**DF**] the cohomology group $H^1(V, L_i)$ is trivial because $(|V|, |L_i|) = 1$, and so $C = V$ as desired. [Proofs of (3) can also be accomplished by more elementary means, such as Maschke's Theorem, etc.!]

We need a lemma that allows us to deal with abstract groups, rather than the groups L_i defined in terms of their specific representations on V.

Lemma. Let M be a subgroup of $GL_2(\mathbb{F}_p)$ isomorphic (as an abstract group) to L_i for some $i \geq 2$. Then $|N_{GL_2(\mathbb{F}_p)}(M) : M| = 2$ when $i < N$ and equals 1 when $i = N$.

Proof: Note that the non-abelian group M acts faithfully, hence also irreducibly, on the 2-dimensional space V. The abstract group M has $Z(M)$ a cyclic group of order $p-1$. Since $\mathbb{F}_p$ contains the $(p-1)^{\text{st}}$ roots of unity, by Schur's Lemma $Z(M)$ consists of scalar matrices, i.e., $Z = Z(M) \leq M$. (Note that Z is represented by scalar matrices for every choice of basis of V.)

Since by (d), $M/Z(M)$ is dihedral of order $2^{i+1}d$, this quotient group has a unique cyclic subgroup of order $2^i d$. Let overbars denote passage to $GL_2(\mathbb{F}_p)/Z = PGL_2(\mathbb{F}_p)$. By (d), both $\overline{L_i}$ and $\overline{M}$ are dihedral of order $2^{i+1}d$, with $Z(\overline{M})$ of order 2. By (g), $|PGL_2(\mathbb{F}_p) : PSL_2(\mathbb{F}_p)| = 2$, and since $i \geq 2$, $Z(\overline{M})$ and $Z(\overline{L_1})$ both belong to $PSL_2(\mathbb{F}_p)$. Also by (g), the latter group has one class of involutions, so we may replace $\overline{M}$ by a conjugate to assume

$$Z(\overline{M}) = Z(\overline{L_i}) := \langle\, \overline{u}\, \rangle.$$

Thus again by (g),

$$\overline{M}, \overline{L_i} \leq C_{PGL_2(\mathbb{F}_p)}(\overline{u}) = \overline{L_N}.$$

In particular, $\overline{M}$ is a dihedral subgroup of order $2^{i+1}d$ in the dihedral group $\overline{L_N}$. The Lemma now follows from (1) together with the remarks following that proof.

We can now finish the proof of (2). By (3), B/V embedds into $GL(V)$, so we may identify B/V as a subgroup of $GL_2(\mathbb{F}_p)$ with A_i/V then identified with some subgroup, B_i, of $GL_2(\mathbb{F}_p)$ isomorphic to L_i as an abstract group. (We do *not* assume that B itself embeds into X.) Under this identification, $A_i/V = B_i \trianglelefteq B/V$. Since $i < N$, by the preceding Lemma applied to $M = B_i$ we get that $|N_{GL_2(\mathbb{F}_p)}(B_i)| = 2|B_i|$. Since $A_i \trianglelefteq A_{i+1} \leq B$ and $|A_{i+1} : A_i| = 2$, we must have $A_{i+1}/V = B/V$ and so $B = A_{i+1}$, as claimed. This completes the main proof.

Thus, starting at $G = A_2$ we get a strictly increasing automorphism tower of length $N-2$:

$$G = A_2 \trianglelefteq A_3 \trianglelefteq \cdots \trianglelefteq A_N \qquad \text{where } A_{i+1} = \mathrm{Aut}(A_i) \text{ and } |A_{i+1} : A_i| = 2, \quad 2 \leq i \leq N-1.$$

Here we chose N *first*, and then *constructed* G (depending on N) to have a tower of length at least $N-2$, which, by Wielandt's Theorem, nonetheless ultimately terminates (see Exercise 3 below).

Remarks:

1. Once we know that $(|V|, |B/V|) = 1$, the extension of B/V by V splits by Schur's Theorem (cf., [**DF**], Section 17.4), independent of knowing that $B = A_{i+1}$; so B embeds into X for this reason as well.

2. Much of this discussion could be simplified by relying on Dickson's list of all subgroups of $PGL_2(\mathbb{F}_p)$ (see [**Di**], XII or [**Hu**], II.7 and 8): Quote these to produce the entire chain of projective subgroups L_i/Z together with identifying their normalizers, take preimages in $GL_2(\mathbb{F}_p)$, and then define the groups $A_i = V \rtimes L_i$ in X to proceed accordingly. We leave it to the reader to write this up!

Exercises

1. Show that if K is the dihedral group of order $2^{N+1} \geq 8$, then $|\mathrm{Aut}(K)| = 2^{2N-1}$.
   [Hint: Use the usual presentation for K and find the number of pairs of generators r', s' that satisfy the "same" (corresponding) relations. (See the end of Section 6.3 of [**DF**].)]
2. Prove, independent of Exercise 1, that $K = D_{2^{N+1}}$ has no nontrivial odd order automorphisms for all $N \geq 2$.
   [Hint: You may quote Burnside's Basis Theorem from Section 6.1 of [**DF**].]
3. In the notation of this example, show that $\mathrm{Aut}(A_N) = A_N$, i.e., the automorphism tower terminates at *exactly* length $N-2$. (Thus, by starting with G equal to some A_k for suitable $k \geq 2$ and "large" enough N, we may construct explicit strictly increasing automorphism towers that terminate in any given positive integer length.)
   [Hint: Likewise V is characteristic in $A_N = L_N$, hence V is normal in $\mathrm{Aut}(A_N)$. Follow the proof of (3).]
4. Prove that $|PGL_2(\mathbb{F}_p) : PSL_2(\mathbb{F}_p)| = 2$.
   [Hint: Every matrix D in $GL_2(\mathbb{F}_p)$ is equivalent mod Z to itself times a scalar matrix. Use this to show that D is equivalent to a matrix whose determinant is a square in $\mathbb{F}_p^\times$; then use that $|\mathbb{F}_p^\times : (\mathbb{F}_p^\times)^2| = 2$.]
5. Prove that $PSL_2(\mathbb{F}_p)$ has no subgroup of index 2, for any odd prime p.
   [Hint: One "group-theoretic" way is to suppose there is some H_1 with $|PSL_2(\mathbb{F}_p) : H_1| = 2$, let $g \in PGL_2(\mathbb{F}_p) - PSL_2(\mathbb{F}_p)$ and let $H = H_1 \cap H_1^g$; so $H \trianglelefteq PGL_2(\mathbb{F}_p)$ and is of index 4 or 8 by the preceding exercise. Use (1) on page 5 to show H must have cyclic Sylow 2-subgroups; then quote Exercise 4.5.49 in [**DF**] to show that H has a normal 2-complement, Y. Deduce that $Y \trianglelefteq PGL_2(\mathbb{F}_p)$, and use that the latter group is doubly transitive on the $p+1$ lines in V to get that Y is transitive on these $p+1$ lines, a contradiction because $p+1$ is even. (Alternatively, Y contains all the $p+1$ Sylow p-subgroups of $PGL_2(\mathbb{F}_p)$.)]
6. Prove that $PSL_2(\mathbb{F}_p)$ has one class of involutions (it is sufficient for our proof that conjugation takes place in $GL_2(\mathbb{F}_p)$ although one could show that $PSL_2(\mathbb{F}_p)$ itself has one class), and that the centralizer in $PGL_2(\mathbb{F}_p)$ of a projective involution in $PSL_2(\mathbb{F}_p)$ is isomorphic to L_N/Z.
   [Hint: One way is to use Jordan canonical forms to show that every element of order 4 in $SL_2(\mathbb{F}_p)$ is conjugate (in $GL_2(\mathbb{F}_p)$) to $u = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, where $i^2 = -1$ in $\mathbb{F}_p$ (u maps to an involution in the projective group); then easily calculate the structure of $N_{GL_2(\mathbb{F}_p)}(\langle\, u \,\rangle)$ either by direct computation or by noting that the latter group permutes the two eigenspaces of u. Another way is to use Thompson's Transfer Lemma, [**DF**] Exercise 17.3.6, together with the preceding exercise.]

References

[Di] *Linear Groups with an Exposition of the Galois Field Theory*, L.E. Dickson, Dover, 1958.

[Hu] *Enliche Gruppen I*, B. Huppert, Springer, 1967.