Crowns in finite groups

A short course for the London Mathematical Society

Gareth Tracey

September 9, 2020

A brief overview

Analogous to the role of the prime numbers in the positive integers, the finite simple groups are the "building blocks" of the finite groups. More precisely, the Jordan-Hölder Theorem states that every finite group G has a *composition series*: That is, a series

$$1 = G_0 < G_1 < \ldots < G_t = G$$

where each G_i is normal in G_{i+1}, and the set $\{G_i/G_{i-1} : 1 \leq i \leq t\}$ of factors consists of simple groups, uniquely determined by G.

Incredibly, we now know all possible isomorphism types of the groups G_{i+1}/G_i. Indeed, the Classification of finite simple groups (henceforth abbreviated to CFSG) is one of the defining achievements of twentieth century mathematics. This incredible theorem has led to numerous breakthroughs in long-standing problems in group theory and beyond, and continues to serve as a vital tool.

What is perhaps less well-known, is that in parallel to the work on the CFSG, the last century (particularly the 1960s and 1970s) saw tremendous progress in the understanding of the finite soluble groups (the dual, in some sense, to the non-abelian finite simple groups). Indeed, as the proof of the CFSG was drawing closer in 1980, H. Wielandt suggested that one of the primary goals for group theorists (using the CFSG or otherwise) should be to extend these wonderful new results on the structure of finite soluble groups to the class of all finite groups.

In this lecture course, we will describe one aspect of this extension: the generalization of the theory of *crowns* in finite soluble groups to the universe of all finite groups. In our first lecture, we will recall some basic facts from group and representation theory, and define the notion of a crown. The second and third lectures will comprise of applications of the theory of crowns: In the second lecture, we will examine the *first cohomology groups* of finite groups acting on vector spaces, and show how the theory of crowns arises naturally in their study. We will also see how this can subsequently be used to count the number of subgroups in a finite group, and the number of isomorphism classes of finite groups of a fixed order. In the final lecture, we will show how information on the crowns in a finite group G can be used to precisely determine the minimal number of elements required to generate G.

Notation and conventions

The following is a list of notation and conventions which will be used throughout the course. Throughout, G is a group.

- The notation $H \leq G$ means that H is a subgroup of G; while $H \trianglelefteq G$ means that H is a normal subgroup of G.
- For a subgroup H of G, G/H denotes the set of right cosets of H in G.
- $C_G(H)$ denotes the centraliser of the subgroup H in G.
- $Z(G)$ denotes the centre of G, while $\Phi(G)$ denotes the Frattini subgroup of G (see Definition 1.3.1).
- $\mathrm{Aut}(G)$ denotes the automorphism group of G.
- For elements x and g of G, we write $x^g = g^{-1}xg$.
- More generally, group actions will always be written on the right. So if the group G acts on the set Ω, we will write ω^g for the image of $\omega \in \Omega$ under the action of $g \in G$.
- For a positive integer k, we will write G^k for the k-fold direct power of G. That is, G^k is the group which, as a set, is the cartesian product of k copies of G, equipped with pointwise multiplication.
- We will write Z_n for the cyclic group of order n, and $\mathbb{F}_p$ for the finite field of order p, for p prime.
- Alt_n and Sym_n will denote the alternating and symmetric groups of degree n, respectively.
- We will write $SL_n(\mathbb{F})$ and $GL_n(\mathbb{F})$ for the special and general linear groups of dimension n over the field $\mathbb{F}$.
- Abelian groups will always be written multiplicatively.

Chapter 1

An introduction to the theory of crowns

Roughly speaking, crowns are certain quotients of finite groups which have a "large" normal subgroup which is isomorphic to a direct product of simple groups. In order to define them rigorously, a number of basic notions from group and representation theory are required. In this chapter, we note these necessary definitions and results. We then conclude (see Section 1.3) by defining an equivalence relation on the set of chief factors of a finite group. This will set us up to define and study the notion of a crown (see Chapter 2).

1.1 Chief factors in finite groups

Recall that for finite groups G and G, $H \leq G$ means that H is a subgroup of G, and $H \trianglelefteq G$ means that H is a normal subgroup of G.

Definition 1.1.1. Let G be a finite group. A *section* of G is a group X/Y, where $X \leq Y$ and $Y \trianglelefteq X$. If X and Y are both normal in G, then we say that X/Y is a *normal section* of G.

Thus, the composition factors in a finite group G are all sections of G, but are not necessarily normal sections. To study crowns in finite groups, we will be interested in the normal sections in G, and specifically the "minimal normal sections". These are called the chief factors of G, and their formal definition is as follows:

Definition 1.1.2. Let G be a finite group. A *chief factor* of G is a normal section X/Y of G with the property that if $Y \leq A \leq X$ with $A \trianglelefteq G$, then $A = X$ or $A = Y$.

The most common (and some of the most important) examples of chief factors of a finite group G are the minimal normal subgroups of G. That is, those normal subgroups N of G with the property that if $A \leq N$ with $A \trianglelefteq G$, then $A = 1$ or $A = N$. These can be seen as chief factors of G by taking $Y := 1$ and $X := N$ in Definition 1.1.2 These groups are particularly important for inductive arguments in finite group theory, and they have a very particular structure:

Lemma 1.1.3. *Let G be a finite group, and let N be a minimal normal subgroup of G. Then $N \cong S^t$ is isomorphic to a direct product of t copies of a finite simple group S.*

Proof. We leave the proof as an exercise for the reader. A reference is.. □

Since a chief factor X/Y of G is a minimal normal subgroup of G/Y, the following is immediate.

Corollary 1.1.4. *Let G be a finite group, and let X/Y be a chief factor of G. Then $X/Y \cong S^t$ is isomorphic to a direct product of t copies of a finite simple group S.*

We finish this section by noting that one can inductively define a series of subgroups of a finite group G as follows: Set $X_0 := 1$, and for $i \geq 1$, let X_i/X_{i-1} be a minimal normal subgroup of the group G/X_{i-1}. We then have a series:

$$1 = X_0 < X_1 < \ldots < X_t = G. \tag{1.1.1}$$

This is a so-called *normal series* (i.e. every group X_i in the series is normal in G, not just in X_{i+1}).

Definition 1.1.5. Let G be a finite group. A series (1.1.1) in G is called a *chief series* for G.

Like a composition series for G, a chief series for G is unique in the following sense: if $1 = X_0 < X_1 < \ldots < X_t$ and $1 = Y_0 < Y_1 < \ldots < Y_s$ are two chief series' for G, then $s = t$ and there is a bijection f from $\{X_i/X_{i-1} : 1 \leq i \leq t\}$ to $\{Y_i/Y_{i-1} : 1 \leq i \leq s\}$ such that $X_i/X_{i-1} \cong f(X_i/X_{i-1})$ for all i. Thus, we may speak of t as the chief length of G, and the set $\{X_i/X_{i-1} : 1 \leq i \leq t\}$ as the set of chief factors of G.

1.2 Representations and the action of a finite group on its chief factors

Suppose that G and A are finite groups, and that G acts on A via $a \to a^g$, $a \in A$, $g \in G$. We say that G acts on A *via automorphisms* if $(ab)^g = a^g b^g$ for all $a, b \in A$, and all $g \in G$. In this case, the map $\theta_g : A \to A$, $a \to a^g$, is an automorphism of A. The associated map $g \to \theta_g$ is a homomorphism from G to $\mathrm{Aut}(G)$, with kernel $C_G(A)$.

For example, a finite group G acts via automorphisms (by conjugation) on any normal section of G. In particular, if X/Y is a chief factor of G and $X/Y \cong S^t$, for a simple group S, we get a well-defined map $G \to \mathrm{Aut}(S^t)$, with kernel $C_G(X/Y)$. The group $G/C_G(X/Y)$ is called the group *induced* by G on X/Y. Since $G/C_G(X/Y)$ is isomorphic to a subgroup of $\mathrm{Aut}(X/Y)$, we will abuse notation and write $G/C_G(X/Y) \leq \mathrm{Aut}(X/Y)$.

We would now like to garner more information on the groups induced by a finite group on its chief factors. Before doing so, we need the following definition:

Definition 1.2.1. Let A be a finite group, and let T be a subgroup of the symmetric group $\mathrm{Sym}(t)$ of degree $t \geq 1$. Then the *(permutational) wreath product* of A by T is the group $A \wr T := A^t \rtimes T$, where the action of T on A^t is defined by

$$(a_1, a_2 \ldots, a_t)^x = (a_{1^{x^{-1}}}, a_{2^{x^{-1}}} \ldots, a_{t^{x^{-1}}}).$$

The subgroups A^t and T are called the *base group* and *top group* of $A \wr T$, respectively.

Definition 1.2.1 will be useful not only for our next lemma, but also for examples throughout the course.

Now let G be a finite group, and let X/Y be a chief factor of G. By Corollary 1.1.4, X/Y is isomorphic to a direct product S^t of t copies of a finite simple group S. Then S is either abelian (i.e. $S \cong Z_p$, for a prime p), or S is a non-abelian simple group. Since the induced group $G/C_G(X/Y)$ is a subgroup of $\mathrm{Aut}(X/Y) \cong \mathrm{Aut}(S^t)$, it will be useful to have information on the automorphism group of a direct product of a non-abelian simple group.

Lemma 1.2.2. *Let S be a finite simple group, $t \geq 1$.*

(i) If S is abelian (i.e. $S \cong Z_p$ for a prime p), then $\mathrm{Aut}(S^t) \cong GL_t(p)$.

(ii) If S is non-abelian, then $\mathrm{Aut}(S^t) \cong \mathrm{Aut}(S) \wr \mathrm{Sym}(t)$.

Recall that a *representation* of a finite group G over a field $\mathbb{F}$ is a homomorphism from G into $GL_n(\mathbb{F})$. We call n the degree of the representation, and the the vector space $\mathbb{F}^n$ is called the *natural module* for G. Lemma 1.2.2(i) states that each abelian chief factor $X/Y \cong Z_p^t$ of a finite group G yields a t-dimensional representation for G over the field $\mathbb{F}_p$ of p elements. Similarly, a permutation representation of a finite group G is a homomorphism from G into $\mathrm{Sym}(n)$, for some $n \geq 1$. The natural number n is called the *degree* of the permutation representation. Lemma 1.2.2(ii) states that each non-abelian chief factor of a finite group G yields a permutation representation for G of degree t.

The following lemma gives more information on the groups induced by a finite group on its chief factors.

Lemma 1.2.3. *Let G be a finite group, and let X/Y be a chief factor of G so that X/Y is isomorphic to a direct product S^t of isomorphic copies of a non-abelian simple group S.*

1. *If S is abelian (i.e. $S \cong Z_p$ for a prime p), then $G/C_G(X/Y) \leq GL_t(\mathbb{F}_p)$ acts irreducibly on the natural module $\mathbb{F}_p^t$.*
2. *If S is non-abelian, then consider the projection $\pi : \mathrm{Aut}(S^t) \cong \mathrm{Aut}(S) \wr \mathrm{Sym}(t) \to \mathrm{Sym}(t)$. Then $\pi(G/C_G(X/Y))$ is a transitive subgroup of $\mathrm{Sym}(t)$.*

Proof. We leave the proof as an exercise for the reader. A reference is.. □

1.3 An equivalence relation on a special set of chief factors of a finite group

Recall that our aim in the first lecture of the course is to define and give some properties for the set of crowns in a finite group G. We are almost ready to do so. But first, we require a standard definition.

Definition 1.3.1. Let G be a finite group.

(i) The *Frattini subgroup*, written $\Phi(G)$, of G is the intersection of all maximal subgroup of G. Thus, $\Phi(G) := \bigcap_{M <_{\max} G} M$.

(ii) A chief factor X/Y of G is called non-Frattini if X/Y is not a subgroup of $\Phi(G/Y)$.

Recall that a finite group G is *nilpotent* if all Sylow subgroups of G are normal in G. The following lemma states, in particular, that $\Phi(G)$ is nilpotent.

Lemma 1.3.2. *Let G be a finite group.*

(i) The subgroup $\Phi(G)$ is nilpotent.

(ii) G is nilpotent if and only if $G/\Phi(G)$ is abelian.

(iii) $\Phi(G)$ is the set of "non-generators". More precisely, $\Phi(G) = \{x \in G : A \subseteq G$ and $\langle x, A\rangle = G$ if and only if $\langle A\rangle = G\}$.

Notice that Lemma 1.3.2(i) implies that every non-abelian chief factor of G is non-Frattini. Suppose then, that X/Y is an abelian chief factor of G. If X/Y is non-Frattini, then G/Y has the form $G/Y = X/Y \rtimes H/Y$, for some subgroup H of G containing Y. Indeed, if X/Y being non-Frattini implies that there exists a maximal subgroup H/Y of G/Y not containing X/Y. Then $G/Y = (X/Y)(H/Y)$. Moreover, $(X/Y) \cap (H/Y)$ is a normal subgroup of G/Y (exercise: why?), and hence must be trivial. Thus, $G/Y = X/Y \rtimes H/Y$, as claimed. For this reason, the non-Frattni chief factors in a finite group are often also called the *complemented* chief factors of G (a complement of a subgroup K in a finite group G is a subgroup K such that $HK = G$ and $H \cap K = 1$).

We would now like to define an equivalence relation on the set of non-Frattini chief factors in a finite group G. We begin with a definition.

Definition 1.3.3. A finite group L is called *monolithic* if L has a unique minimal normal subgroup N. If in addition N is not contained in $\Phi(L)$, then L is called a *monolithic primitive group*.

The reason for the terminology "primitive" in Definition 1.3.3 is that if $N \not\leq \Phi(L)$, then there exists a maximal subgroup M of L which does not contain N. It follows that M is core-free in L, and hence that L has a faithful primitive permutation action on the cosets of M.

Our next definition introduces the "crown" terminology:

Definition 1.3.4. Let L be a monolithic primitive group and let N be its unique minimal normal subgroup. For each positive integer k, let L^k be the k-fold direct product of L. The *crown-based power of L of size k* is the subgroup L_k of L^k defined by

$$L_k = \{(l_1, \dots, l_k) \in L^k \mid l_1 \equiv \dots \equiv l_k \ \mathsf{mod} N\}.$$

Equivalently, $L_k = N^k \operatorname{diag}(L^k)$.

Our next lemma gives more information about the groups L_k.

Lemma 1.3.5. *Let L be primitive monolithic, with minimal normal subgroup N, and let k be a positive integer. Recall that if N is abelian then N has a complement, say H, in L. Set $H^* := \mathrm{diag}(H^k) \leq L^k$. Then*

(i) H^* is a complement to N^k in L_k; and

(ii) $C_{H^*}(N^k)$ is trivial.

This will be important.

We are now almost ready to define the equivalence relation on chief factors in finite groups mentioned at the beginning of the section. First, recall that if a group G acts on a group V via automorphisms, then we say that V is a *G-group*. As we saw earlier, the most widely studied G-groups are the groups of the form $V = \mathbb{F}^n$, for some field $\mathbb{F}^n$: these are the $\mathbb{F}[G]$-modules, and the associated maps $G \to \mathrm{Aut}(V) \cong GL_n(\mathbb{F})$ are the $\mathbb{F}[G]$-representations. Our next definition generalises some basic notions in representation theory to arbitrary G-groups.

Definition 1.3.6. Let G be a finite group, and let V and W be G-groups.

(i) If G does not stabilise any non-trivial subgroup of V, then V is called an *irreducible* G-group.

(ii) If there exists an isomorphism $f : V \to W$ such that $f(v)^g = f(v^g)$ for all $g \in G$, then V and W are said to be G-isomorphic.

We are now ready to define G-equivalent G-groups:

Definition 1.3.7. Let G be a finite group. We say that two irreducible G-groups V_1 and V_2 are *G-equivalent* and we put $V_1 \sim_G V_2$, if there are isomorphisms $\phi : V_1 \to V_2$ and $\Phi : V_1 \rtimes G \to V_2 \rtimes G$ such that the following diagram commutes:

$$\begin{tikzcd}
1 \arrow[r] & V_1 \arrow[r] \arrow[d, "\phi"] & V_1 \rtimes G \arrow[r] \arrow[d, "\Phi"] & G \arrow[r] \arrow[d, "id"] & 1 \\
1 \arrow[r] & V_2 \arrow[r] & V_2 \rtimes G \arrow[r] & G \arrow[r] & 1.
\end{tikzcd} \tag{1.3.1}$$

Note that the two rows in the diagram (1.3.1) represent standard short exact sequences. That is, $V_i \to V_i \rtimes G$ is the usual inclusion map, while $V_i \rtimes G \to G$ is the quotient map by V_i (so $v_i g$ gets sent to g, for $v_i \in V_i$, $g \in G$).

The following lemma shows that being G-equivalent is weaker than being G-isomorphic.

Lemma 1.3.8. *Let G be a finite group, and let V_1 and V_2 be G-groups.*

(i) If V_1 and V_2 are G-isomorphic, then V_1 and V_2 are G-equivalent.

(ii) In the particular case where V_1 and V_2 are abelian the converse is true: if V_1 and V_2 are abelian and G-equivalent, then V_1 and V_2 are also G-isomorphic.

Proof. Part (i) is easy: if $f : V_1 \to V_2$ is a G-isomorphism, then define the isomorphisms ϕ and Φ from Definition **??** by $\phi := f$ and $\Phi : V_1 \rtimes G \to V_2 \rtimes G$, $v_1 g \to f(v_1)g$. Is it straightforward to check that these maps are indeed isomorphisms. It is then trivial to see that the diagram (1.3.1) commutes.

For part (ii), assume that V_1 and V_2 are abelian, and that V_1 and V_2 are G-equivalent. Let ϕ and Φ be the maps from Definition **??**. We claim that $\phi : V_1 \to V_2$ is in fact a G-isomorphism. Indeed, fix $g \in G$, and let v_1 be an element of V_1. Then using the commuting diagram (1.3.1), we have

$$\phi(v_1^g) = \Phi(v_1^g) = \Phi(v_1)^{\Phi(g)}, \tag{1.3.2}$$

where the last equality follows since Φ is a group homomorphism. The diagram (1.3.1), however, implies that $\Phi(g) = ug$, for some $u \in V_1$. Since V_1 is abelian, we deduce from (1.3.2) that $\phi(v_1^g) = \Phi(v_1)^g$. Since $\Phi\downarrow_{V_1}= \phi$, it follows that ϕ is a G-isomorphism, as claimed. □

Remark 1.3.9. Note that if two G-groups V_1 and V_2 are G-isomorphic, then it follows from the definition of G-isomoprhism that $C_G(V_1) = C_G(V_2)$. This is often a quick and easy way to show that two G-groups are not G-isomorphic.

The following is an example where two G-groups are G-equivalent, but not G-isomorphic:

Example 1.3.10. Let $G = \mathrm{Alt}_5 \times \mathrm{Alt}_5$, and let V_1 and V_2 be the normal subgroups $V_1 := \mathrm{Alt}_5 \times 1$, $V_2 := 1{\times}_5$. Then $C_G(V_1) = V_2$ and $C_G(V_2) = V_1$, so V_1 and V_2 are not G-isomorphic (see Remark 1.3.9).

On the other hand, define $\phi : V_1 \to V_2$ by $\phi((x, 1)) = (1, x)$, and $\Phi : V_1 \rtimes G \to V_2 \rtimes G$ by $\Phi((x, 1)(g, h)) = (1, x)(1, gh^{-1})(g, h)$. Then it is a routine exercise to check that ϕ and Φ are isomorphisms, and the associated diagram as at (1.3.1) commutes.

Chapter 2

Equivalence classes of non-Frattini chief factors in a finite group

In this chapter, our aim is two-fold: first, we will build on our work in Chapter 1 to define the *set of crowns* of a finite group G. Secondly, we will demonstrate how this set of crowns can be used to determine precisely the minimal number of elements required to generate G.

2.1 Primitive permutation groups

As Definition 1.3.3 suggests, primitive permutation groups play an important role in the theory of crowns in a finite group. In this section, we will briefly recall some important notions from permutation group theory, and in particular, from the theory of primitive groups.

First, recall from Section **??** that a *permutation group on a set* Ω is a subgroup G of the symmetric group $\mathrm{Sym}(\Omega)$. In this case, Ω is called a *G-set*. If Ω is finite of cardinality n, then we say that G is a *permutation group of degree* n. Recall also that if G is a finite group acting on a set Ω, then the associated homomorphism $G \to \mathrm{Sym}(\Omega)$ is called a *permutation representation* of G.

As with G-groups, we have a notion of isomorphism between G-sets.

Definition 2.1.1. Let G be a finite group. Two G-sets Ω_1 and Ω_2 are said to be *G-isomorphic* if there is a bijection $f : \Omega_1 \to \Omega_2$ such that $f(\omega_1^g) = f(\omega_1)^g$ for all $\omega_1 \in Omega_1$, $g \in G$.

The following are special types of permutation representations.

Definition 2.1.2. Let G be a finite group acting on a finite set Ω.

1. G is said to act *transitively* on Ω if for all $\omega_1, \omega_2 \in \Omega$, there exists $g \in G$ such that ${}_1^g = \omega_2$.

2. G is said to act *primitively* on Ω if G acts transitively on Ω and a point stabiliser $G_\omega = \{g \in G : \omega^g = \omega\}$ is a maximal subgroup of G.

The following are basic, but important remarks about transitive and primitive permutation representations of a finite group.

Remark 2.1.3. Suppose that G is a finite group acting transitively on a finite set Ω.

1. All point stabilisers are G-conjugate, so if one point stabiliser is maximal in G, then they all are.
2. Consider the G-set G/G_ω (i.e. the set of right G-cosets of G_ω, acted upon by G by right multiplication). Then the G-sets Ω and G/G_ω are G-isomorphic. Thus, each transitive permutation representation of a finite group G may be viewed as the action on the set of right cosets of a subgroup. In particular, each primitive permutation representations of G can be viewed as the actions on the set of right cosets of a maximal subgroup of G.
3. The kernel K of the action of G on Ω is the *core* of G_ω in G. That is, $K = \bigcap_{g\in G} G_\omega^g$.

A famous result, due independently to O'Nan and Scott, characterises the primitive permutation groups into types, usually based on geometric considerations. In this course, we will only be concerned with one of these types, which we now define.

Definition 2.1.4. A primitive permutation group G is said to have *simple diagonal type* if there exists a nonabelian finite simple group T such that

(i) $T \times T \leq G \leq \mathrm{Aut}(T) \times \mathrm{Aut}(T)$; and

(ii) $G_\omega \cap (T \times T)$ has the form

$$G_\omega \cap (T \times T) = \{(t, t^\alpha) : t \in T\}$$

for some $\alpha \in \mathrm{Aut}(T)$.

Note that a primitive permutation group of simple diagonal type as in Definition 2.1.4 above has two minimal normal subgroups, each isomorphic to T.

Remark 2.1.5. If T is a finite simple group, then a subgroup H of the k-fold direct power T^k is said to be a *diagonal subgroup* if H ahs the form

$$H = \{(t, t^{\alpha_2}, \ldots, t^{\alpha_k}) : t \in T\}$$

for some automorphisms $\alpha_i \in \mathrm{Aut}(T)$. Thus, in this language a primitive permutation group has simple diagonal type if there exists a finite simple group T such that $T \times T \leq \mathrm{Aut}(T) \times \mathrm{Aut}(T)$, and a point stabiliser in G intersects $T \times T$ in a diagonal subgroup.

2.2 Back to equivalence classes of chief factors

Now, we have already seen an example of a primitive permutation group of simple diagonal type. Namely, take G to be as in Example [**?**] (so $T = \mathrm{Alt}_5$), and take Ω to be the set of right cosets of the diagonal subgroup $\{(t,t) : t \in \mathrm{Alt}_5\}$.

For our purposes, the important thing about this group was that it gave us an example of a finite group G with G-equivalent chief factors which are not G-isomorphic. We have seen already that two abelian chief factors of G are G-isomorphic if and only if they are G-isomorphic. By a result of Jiménez-Seral and Lafuente, the non-Frattini chief factors in a finite group which are G-equivalent but not G-isomorphic occur in a very similar way to Example **??**:

Proposition 2.2.1. *Let G be a finite group, and let V_1 and V_2 be non-Frattini chief factors of G. Then V_1 and V_2 are G-equivalent if and only if one of the following holds:*

(i) V_1 and V_2 are G-isomorphic; or

(ii) G has a maximal subgroup M such that $G/\operatorname{core}_G(M)$ is a primitive permutation group of simple diagonal type, with minimal normal subgroups G-isomorphic to V_1 and V_2.

Now, Proposition 2.2.1 gives us a useful way to determine the equivalence classes of chief factors in a finite group. Some important examples are as follows.

Example 2.2.2. Let G be a finite p-group, for p prime. Then the non-Frattini chief factors of G all occur in $G/\Phi(G)$ - an elementary abelian p-group. Thus, all non-Frattini chief factors of G are G-isomorphic to the trivial G-group $\mathbb{F}_p$.

Example 2.2.3. Let L be a primitive monolithic group with minimal normal subgroup N, and let $G = L_k$ be the crown based power of length k (see Definition **??**). By Lemma **??**, $G = N^k \operatorname{diag}(L^k)$. In particular, each element of G can be written uniquely in the form $g = (l, n_2l, \ldots, n_kl)$, for $l \in L$ and $n_i \in N$.

For $1 \leq i \leq k$, let V_i be the ith coordinate subgroup of N^k. That is,

$$V_i := \{(1, \ldots, 1, \underbrace{v_i}_{i\text{th position}}, 1 \ldots, 1) : v_i \in N\}.$$

We claim that V_i is G-equivalent to V_j for all i, j. Indeed, for fixed $1 \leq i, j \leq k$, define $\phi : V_i \to V_j$ by $\phi(1, \ldots, 1, \underbrace{v_i}_{i\text{th position}}, 1 \ldots, 1) = \phi(1, \ldots, 1, \underbrace{v_i}_{j\text{th position}}, 1 \ldots, 1)$; and define $\Phi : V_i \rtimes G \to V_j \rtimes G$ by $\phi(1, \ldots, 1, \underbrace{v_i}_{i\text{th position}}, 1 \ldots, 1)(l, n_2l, \ldots, n_kl) = \phi(1, \ldots, 1, \underbrace{v_in_j^{-1}}_{j\text{th position}}, 1 \ldots, 1)(l, n_2l, \ldots, n_kl)$.

It is routine (though non-trivial) to prove that ϕ and Φ are homomorphisms, and that the associated diagram as at (1.3.1) commutes. Thus, all V_i and V_j are G-equivalent.

The following is an illustration of how one finds representatives for the equivalence classes of non-Frattini chief factors of G in a specific example.

Example 2.2.4. Consider $G = \operatorname{Sym}_4$. Since G is soluble, two chief factors V_1 and V_2 are G-equivalent if and only if they are G-isomorphic. Now, a chief series for G is

$$1 < V_4 < \underset{4}{\operatorname{Alt}} < G$$

where $V_4 = \langle (1,2)(3,4), (1,3)(2,4) \rangle$. Since G, $G/V_4 \cong \operatorname{Sym}_3$, and $G/\operatorname{Alt}_4 \cong Z_2$ all have trivial Frattini subgroups (exercise: prove this), each of associated chief factors are non-Frattini. Furthermore, finding a set of representatives for the G-equivalence classes of Frattini chief factors for G is easy in this case, since the chief factors V_4, Alt_4/V_4, and G/Alt_4 are pairwise non-isomorphic as groups, so are certainly pairwise non isomorphic as G-groups. Thus, $\{V_4, \mathrm{Alt}_4/V_4, \mathrm{Sym}_4/\mathrm{Alt}_4\}$ is a complete set of representatives for the G-equivalence classes of choef factors in $G = \mathrm{Sym}_4$.

Find a set of representatives for the non-Frattini chief factors in the cases $G = GL_2(3)$ and $G = Z_p \rtimes Z_{p-1}$, where p is prime and Z_{p-1} acts on Z_p as $\mathrm{Aut}(Z_p)$.

2.3 The set of crowns in a finite group

In this section, we will finally be able to define the set of crowns in a finite group G. As the terminology suggests, and as the next lemma shows, crown based powers play an important role in this definition:

Lemma 2.3.1. *Let G be a finite group, and let V be a non-Frattini chief factor of G. Then:*

(i) There exists a maximal subgroup M of G such that $G/\mathrm{core}_G(M)$ has a minimal normal subgroup G-isomorphic to V.

(ii) Set $R_G(V) := \bigcap_M \mathrm{core}_G(M)$, where the intersection runs over all maximal subgroups M of G such that $G/\mathrm{core}_G(M)$ has a minimal normal subgroup G-isomorphic to V. Also, define $L := G/C_G(V)$ if V is non-abelian and $L := V \rtimes (G/C_G(V))$ otherwise. Then $G/R_G(V) \cong L_k$, where k is the number of non-Frattini chief factors in any chief series for G which are G-equivalent to V.

Proof. Let $Y \leq X$ be normal subgroups of G with $V = X/Y$. Since V is non-Frattini, we may choose a maximal subgroup M of G containing Y so that M/Y does not contain $V = X/Y$. We deduce in particular that $X/Y \not\leq \mathrm{core}_G(M)/Y$ (note that $Y \leq \mathrm{core}_G(M)$, since $\mathrm{core}_G(M)$ is the largest normal subgroup of G contained in M). Since X/Y is a minimal normal subgroup of G/Y, we must then have $X \cap \mathrm{core}_G(M) \leq Y$, and so $X \cap \mathrm{core}_G(M) = Y$. Now define $f : X/Y \to X\,\mathrm{core}_G(M)/\mathrm{core}_G(M)$ by $f(Yx) := (\mathrm{core}_G(M)x)$. Since $X \cap \mathrm{core}_G(M) = Y$, it follows quickly that f is a G-isomorphism. This proves (i).

We now prove (ii) by induction on k. If $k = 1$, then $G/R_G(V)$ is isomorphic to $L \cong L_1$ by part (i) above. So assume that $k > 1$ and that the result holds for groups which have strictly less than k non-Frattini chief factors equivalent to V. Then we may choose a normal subgroup N of G such that G/N has precisely $k-1$ non-Frattini chief factors G-equivalent to V, and such that precisely one non-Frattini G-chief factor contained in N is G-equivalent to V. Set $R = \bigcap_M \mathrm{core}_G(M)$, where M runs over the set of maximal subgroups of G containing N with the property that $G/\mathrm{core}_G(M)$ has a minimal normal subgroup G-isomorphic to V. Then $R/N = R_{G/N}(V)$, so the inductive hypothesis guarantees that $G/R \cong L_{k-1}$.

Now, let X/Y be a non-Frattini chief factor of G which is G-equivalent to V, and such that $Y \leq X \leq N$. By construction, R acts trivially on a chief factor of G which is G-equivalent to V. Thus, by Lemma **??**, R is either contained in $C_G(V)$, or R has a factor group R/S with $S \trianglelefteq G$

such that R/S is G-equivalent to V. In the former case, V must be abelian. Hence, since $X/Y \leq Z(R/Y)$ and X/Y intersects $\Phi(R/Y) \leq \Phi(G/Y)$ trivially, we must have $[R,R] \leq Y < X \leq R$. Since $R/[R,R]$ modulo $(R/[R,R]) \cap \Phi(R/[R,R])$ is a direct product of non-Frattini chief factors of G, and R contains a unique chief factor of G which is G-equivalent to V, we deduce that R has a subgroup S containing $[R,R]$ such that $S \trianglelefteq G$ and $R/S \sim_G V$.

Thus, in either case, R has a subgroup S, with S normal in G, such that $R/S \sim_G V$. Since $I/R \cong V^{k-1}$, R/S commutes with I/R, and R/S is not in $\Phi(I/S)$, it follows that $I/S \cong V^k$. Since $G/I \cong G/C_G(V)$, it follows that $G/S \cong L_k$. The result now follows. □

Lemma 2.3.1 is the key lemma in the theory of crowns, and allows us to define the following:

Definition 2.3.2. Let G be a finite group, and let V be a non-Frattini chief factor of G.

1. The normal subgroup $R_G(V)$ from Lemma 2.3.1 is called the V*-core* of G.
2. The subgroup $I_G(V)$ is defined so that $I_G(V)/R_G(V) = (G/R_G(V))$. We call $I_G(V)/R_G(V)$ the V*-crown* of G.
3. As proved in Lemma 2.3.1, $I_G(V)/R_G(V) \cong V^k$. We define $\delta_G(V) := k$, so that $\delta_G(V)$ is the number of non-Frattini chief factors G-equivalent to V in any chief series for G.

We can now define the set of *crowns* in a finite group G.

Definition 2.3.3. Let G be a finite group. The set $\{I_G(V)/R_G(V) : V \text{ a non-Frattini chief factor of } G\}$ is called the *set of crowns for* G.

Chapter 3

Applications of crowns: Minimal generator numbers and cohomology

In this chapter, our aim is to demonstrate two of the most useful applications of the theory of crowns to problems in finite group theory. Specifically, these problems are: (1) finding the minimal number of elements required to generate a finite group G; and (2) finding the order of the first cohomology group of G with respect to some module for G. We begin with the former.

3.1 Application 1: Minimal generator numbers in finite groups

For a finite group G, define $d(G) := \min\{|X| : \langle X\rangle = G\}$ to be the minimal size of a generating set for G. Thus, if G is cyclic, for example, then $d(G) = 1$. If V is an elementary abelian group of dimension n over a finite prime field $\mathbb{F}_p$, then $d(G)$ is just the $\mathbb{F}_p$-dimension of G: that is, $d(G) = n$.

The last example shows that the function d is well-behaved when G is a vector space: namely, $d(H) \leq d(G)$ when H is a subgroup (i.e subspace) of G. But this is far from true in general:

Remark 3.1.1. If G is a finite group, then it is not true in general that $d(H) \leq d(G)$ for a subgroup H of G. For example, take G to be the wreath product $R \wr S$ (see Definition 1.2.1) where $R \cong S \cong Z_p$. The base group $H \cong R^p$ of G is elementary abelian of order p^p, and so $d(H) = \dim_{\mathbb{F}_p}(H) = p$. However, if we set $X := \{(r, 1 \ldots, 1)_p, s\}$, where r is a generator for R and s is a generator for $S \leq R \wr S$, then it is easy to see that $G = \langle X\rangle$. Thus, $d(G) = 2$, since G is not cyclic.

The above example shows that there can be no bound on $d(H)$ in terms of $d(G)$ for subgroups H of a finite group G, even for finite p-groups.

Finite p-groups are, however, quite straightforward to deal with when it comes to finding $d(G)$, as the next result shows.

Proposition 3.1.2. *Let G be a finite group. Then $d(G) = d(G/\Phi(G))$. In particular, if G is a finite p-group, for p prime, then $d(G)$ is the dimension of the $\mathbb{F}_p$-vector space $G/\Phi(G)$.*

Proof. That $d(G) \leq d(G/\Phi(G))$ follows immediately from Lemma 1.3.2 (since $\Phi(G)$ is the set of "non-generators" for G). On the other hand, if X is a genrating set for G, and N is any normal subgroup of G, then the set $\{Nx : x \in X\}$ is a generating set for G. Hence $d(G/N) \leq d(G)$. In particular, $d(G/\Phi(G)) \leq d(G)$, so $d(G) = d(G/\Phi(G))$. □

Example 3.1.3. Recall from Example 2.2.2 that a finite p-group has a unique G-equivalence of non-Frattini chief factors, represented by the trivial $\mathbb{F}_p[G]$-module $V := \mathbb{F}_p$. Since all non-Frattini chief factors of G occur as chief factors of $G/\Phi(G)$, and all chief factors of $G/\Phi(G)$ are non-Frattini, we deduce that G has precisely $d(G)$ non-Frattini chief factors of G (all G-equivalent to V). Since G acts trivially on V, we have $L_V = V$ (where L is as in Lemma 2.3.1), and so $G/R_G(V) \cong V^{d(G)} \cong (\mathbb{F}_p)^{d(G)}$. In particular, $R_G(V) = \Phi(G)$ and $\delta_G(V) = d(G)$ in this case.

Remark 3.1.4. During the course of the proof of Proposition 3.1.2, we proved that if G is a finite group and N is a normal subgroup of G, we have $d(G/N) \leq d(G)$. A useful and often used inductive tool is the (almost trivial) upper bound $d(G) \leq d(G/N) + d(N)$.

As mentioned in Example 3.1.3, we have $d(G) = d(G/R_G(V))$ for a finite p-group G, where V is the (up to G-equivalence) unique non-Frattini chief factor of G. The next result shows that this (perhaps surprisingly) can be made more general.

Theorem 3.1.5. *[**?**, Theorems 1.4 and 2.7] Let G be a finite group with $d(G) \geq 3$. Then G has a non-Frattini chief factor V such that $d(G) = d(G/R_G(V))$. Moreover:*

1. *if G is abelian, then $d(G) = d(G/R_G(V)) \leq \delta_G(V) + 1$;*
2. *if G is nonabelian, then $d(G) = d(G/R_G(V)) \leq \log_{|V|}(\delta_G(V)) + 1$.*

The proof of Theorem 3.1.5 is beyond the scope of this course, but we refer the interested reader to [**?**, Theorems 1.4 and 2.7] for details.

Theorem 3.1.5 is an incredibly useful tool for determining the minimal generator numbers in various classes of finite groups. We illustrate this with some examples.

Example 3.1.6. Let $G = T^k$ be the k-fold direct power of a nonabelian finite simple group T. As mentioned in Remark 3.1.4, we have $d(G) \leq d(G/N)$ for any normal subgroup N of G. Hence, since every finite simple group can be generated by 2 elements, we have $d(G) \leq 2k$.

Let us see if we can do any better using the theory of crowns: First, note that G is isomorphic to the crown based bower T_k, and so G has a unique equivalence class of non-Frattini chief factors, isomorphic to T, by Example 2.2.3. Clearly, $\delta_G(T) = k$. Hence, Theorem 3.1.5 yields $d(G) \leq \log_{|T|}(k) + 1$ - a far tighter bound than $d(G) \leq 2k$.

Example 3.1.7. Let G be the wreath product $R \wr S$, where $R = Z_p$ is cyclic of prime order p, and $S = \mathrm{Alt}_s$ is the alternating group of degree $s \geq 5$. Consider the following subgroups of the base group R^s of G:

$$V_1 := \{(x, x, \ldots, x) : x \in R\} \text{ and } V_2 := \{(x_1, x_2, \ldots, x_s) : x_i \in R, \prod_{i=1}^{s} x_i = 1\}.$$

The subgroups V_1 and V_2 are clearly normal in G. Since $|V_1| = p$, V_1 is a minimal normal subgroup of G. Note that $V_1 \leq V_2$ if $p \mid s$, and $V_1 \not\leq V_2$ otherwise. Since V_2 has order p^{s-1}, we deduce that $V_1V_2 = V_2$ has index p in R^s if $p \mid s$, and $V_1V_2 = R^s$ otherwise. It is not difficult to prove (see [**?**, Proposiiton 5.4.1]) that Alt_s acts irreducibly on the $\mathbb{F}_P[\mathrm{Alt}_s]$-module V_1V_2/V_1, and hence that V_1V_2/V_1 is a chief factor of G. Thus, since $G/R^s \cong \mathrm{Alt}_s$ is simple, we deduce that

$$1 < V_1 < V_1V_2 \leq R^s < G$$

is a chief series for G. Since $|V_1V_2/V_1| = p^{s-2}$ if $p \mid s$, and $|V_1V_2/V_1| = p^{s-1}$ otherwise, we have that G has two chief factors G-isomorphic to the trivial $\mathbb{F}_p[G]$-module $\mathbb{F}_p$ if $p \mid s$, and one chief factor G-isomorphic to $\mathbb{F}_p$ otherwise. Hence, $\delta_G(\mathbb{F}_p) \leq 2$. Furthermore, we clearly have $\delta_G(V_1V_2/V_1) = 1$, and $\delta_G(\mathrm{Alt}_s) = 1$. In fact, it is not difficult to prove that if $p \mid s$, then $V_1 \leq \Phi(G)$, so $\delta_G(V) = 1$ for all non-Frattini chief factors V of G. Hence, Theorem 3.1.5 yields $d(G) \leq 2$. Thus, $d(G) = 2$, since G is not cyclic.

Bibliography

[1] A. Ballester-Bolinches and L. M. Ezquerro, Classes of finite groups, Mathematics and Its Applications (Springer), vol. 584, Springer, Dordrecht, 2006.

[2] P. J. Cameron, Permutation groups, London Math. Soc. (Student Texts), vol. 45, CUP, Cambridge, 1999.

[3] F. Dalla Volta and A. Lucchini, Finite groups that need more generators than any proper quotient, J. Austral. Math. Soc., Series A, 64, (1998) 82–91.

[4] E. Detomi and A. Lucchini, Crowns and factorization of the probabilistic zeta function of a finite group, J. Algebra, 265 (2003), no. 2, 651–668.

[5] J. D. Dixon, Random sets which invariably generate the symmetric group, Discrete Math 105 (1992) 25-39.

[6] W. Gaschütz, Praefrattinigruppen, Arch. Mat. 13 (1962) 418–426.

[7] R. Guralnick and C. Hoffman, The first cohomology group and generation of simple groups, Proceedings of the Conference on Groups and Geometries, Siena, September 1996 (eds. L. Di Martino, W.M. Kantor, G. Lunardon, A. Pasini and M.C. Tamburini, Birkhäuser, Basel) (1998), 149–153.

[8] D.F. Holt and C.M. Roney-Dougal, Minimal and random generation of permutation and matrix groups, J. Algebra 387 (2013), 195–223.

[9] I. M. Isaacs, Finite Group Theory, Graduate Studies in Mathematics, vol. 92, American Mathematical Society, Providence, 2008.

[10] P. Jiménez-Seral and J. Lafuente, On complemented nonabelian chief factors of a finite group, Israel J. Math. 106 (1998), 177–188.

[11] W. M. Kantor, A. Lubotzky and A. Shalev, Invariable generation and the Chebotarev invariant of a finite group, J. Algebra 348 (2011), 302–314.

[12] W. Kimmerle, R. Lyons, R. Sandling and D. N. Teague, Composition factors from the group ring and Artin's theorem on orders of simple groups, Proc. London Math. Soc. (3) 60 (1990), no. 1, 89–122.

[13] E. Kowalski and D. Zywina, The Chebotarev invariant of a finite group, Exp. Math. 21 (2012), no. 1, 38–56.

[14] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, J. Algebra 32 (1974), 418–443.

[15] M. Liebeck, L. Pyber and A. Shalev, On a conjecture of G.E. Wall. J. Algebra 317 (2007), 184–197.

[16] A. Lucchini, The Chebotarev invariant of a finite group: A conjecture of Kowalski and Zywina, Proc. Amer. Math. Soc. 146 (11) (2018), 4549–4962.

[17] A. Lucchini, F. Menegazzo and M. Morigi, On the number of generators and composition length of finite linear groups, J. Algebra 243 (2001), 427–447.

[18] A. Lucchini and G. Tracey, An upper bound on the Chebotarev invariant of a finite group, Israel J. Math. 219 (1) (2017), 449–467.

[19] G. Seitz and A. Zalesskii, On the minimal degrees of projective representations of the finite Chevalley groups II, J. Algebra 158 (1993), no. 1, 233–243.

[20] U. Stammbach, Cohomological characterisations of finite solvable and nilpotent groups, J. Pure Appl. Algebra 11 (1977/78), no. 1–3, 293–301.

[21] P. H. Tiep, Low dimensional representations of finite quasisimple groups, Groups, combinatorics and geometry (Durham, 2001), 277–294, World Sci. Publ., River Edge, NJ, 2003.