Finite Simple Groups

Lecture Notes

Sergey Shpectorov

January 22, 2007

1 Introduction: Goals of the course

Finite simple groups are building blocks out of which all finite groups are made. Abelian simple groups are the cyclic groups of prime order, $\mathbb{Z}_p$, and they are discussed in every introductory abstract algebra course. In contrast, nonabelian finite simple groups are much more complicated objects and they are virtually never (with the possible exception of the *alternating groups* $\mathrm{Alt}(n)$) discussed in any detail in any undergraduate courses. This is regretful since simple groups play such a fundamental role in the finite group theory.

Just like all abelian simple groups can be explicitly listed (they are the $\mathbb{Z}_p$'s!), the nonabelian finite simple groups can also be listed, that is, they have been *classified*. The completion of the classification was announced in 1981, this was a concerted effort of a large number of mathematicians and the proof of the classification theorem is spreads in several hundreds (by some estimates, around 600) of journal articles with the total length of several thousand pages (by the same estimates, around 15 thousand pages).

Theorem 1.1 (CFSG) *Every finite simple group is (isomorphic to) one of the following:*

(a) *a cyclic group $\mathbb{Z}_p$, p a prime number;*

(b) *an alternating group* $\mathrm{Alt}(n)$, $n \geq 5$*;*

(c) *a simple* group of Lie type*;*

(d) *one of the* 26 sporadic simple groups.

Since the groups in (a) and (b) are probably familiar, we only need to discuss the groups of Lie type and sporadic groups.

Another name for the groups of Lie type is *Chevalley groups*. These groups form the bulk of all finite simple groups. There are six two-parameter and ten one-parameter families of Chevalley groups. Here are their standard names: $A_n(q)$, $B_n(q)$, $C_n(q)$, $D_n(q)$, ${}^2A_n(q)$, ${}^2D_n(q)$, $E_n(q)$, $n = 6, 7$, and 8, $F_4(q)$, $G_2(q)$, ${}^2B_2(q)$, $q = 2^n$, ${}^3D_4(q)$, ${}^2E_6(q)$, ${}^2F_4(q)$, $q = 2^n$, and ${}^2G_2(q)$, $q = 3^n$. The parameter n is called the *rank* parameter, and q, which is always a prime power, $q = p^a$, is called the *field* parameter. The prime p is called the *characteristic*.

Of course, this notation does not tell you what these groups really are, but at least it gives you an idea of how many of them exist.

Some of the Chevalley groups arise as the so-called *classical groups*. An example of this is the Chevalley group $A_n(q)$, which is nothing but the classical group $\mathrm{PSL}(n+1, q)$, the projective special linear group of dimension $n+1$ over the finite field of order q. The general linear group $\mathrm{GL}(d, q)$ is the group of all invertible $d \times d$ matrices with entries in the finite field $GF(q)$ of size q. The special linear group $\mathrm{SL}(d, q)$ is the normal subgroup of $\mathrm{GL}(d, q)$ consisting of all matrices of determinant one. The projective special linear group $\mathrm{PSL}(d, q)$ is the factor group of $\mathrm{SL}(d, q)$ over the normal subgroup consisting of all scalar matrices of determinant one.

The classical group setup is more concrete and easier to work with, but it does not cover all groups of Lie type and also it depends on the type of the group. The Chevalley group setup is a lot more abstract, but it has the advantage of uniformity, that is, it allows to study all Chevalley groups at once.

The sporadic simple groups are the groups that are not members of any infinite families, so each of them forms an individual unit on the list. Here is the complete list of sporadic simple groups: Mathieu groups M_{11}, M_{12}, M_{22}, M_{23}, and M_{24}, Janko groups J_1, J_2, J_3, and J_4, Conway groups Co_1, Co_2, and Co_3, Fischer groups $F(22)$, $F(23)$, $F(24)$, F_1, F_2, Higman-Sims group HS, Held group He, Rudvalis group Ru, McLaughlin group McL, O'Nan group $O'N$, Lyons group Ly, Harada-Norton group HN, Suzuki group Suz, and Thompson group Th.

The sporadic groups are typically called after their discoverer(s). In this respect, we should mention that J_2 is also called the Hall-Janko group and

$O'N$ is also called the O'Nan-Sims group. The two largest sporadic groups are the groups F_2 and F_1. Because of their size, they have special names: F_1 is called the Fischer-Griess *Monster* and F_2 is called the *Baby Monster*. They also have alternative notation: M for the Monster and BM for the Baby Monster. The Monster is the largest, with approximately 10^{84} elements. It has been mentioned that this number is greater than the number of atoms in the visible universe. Interestingly, the Monster group arises in physics applications, namely in quantum physics.

Note though that, however huge the size of the Monster group may seem, the serial simple groups (prime cyclic, alternating and Lie type) are larger than any sporadic groups once the parameters p, n, and q are sufficiently large.

We can now set the *goals of this course*. Not being able in such a short time to discuss any significant part of the classification, we will concentrate on the groups themselves and on their properties. Again, because of the time limitations, we cannot discuss, or even define all finite simple groups, so we will discuss a few of each type. We will also see how these groups arise as groups of symmetries of various combinatorial and geometric objects. By studying the properties of these objects we can discover the properties of the groups that act on them.

2 Simple groups, abelian simple groups

We start by refreshing a few concepts from the introductory group theory course. Suppose G is a group and $g \in G$.

Definition 2.1 (conjugation) *The mapping $c_g : G \to G$ defined by $h \mapsto g^{-1}hg$ is called conjugation by g.*

We will denote the expression $g^{-1}hg$ by h^g (so-called *exponential notation* for conjugation). More generally, if $H \subseteq G$ then H^g denotes the set $\{h^g \mid h \in H\}$.

Definition 2.2 (normal subgroup) *Suppose $H \leq G$, that is, H is a subgroup of G. We say that H is normal in G and write $H \trianglelefteq G$ if $H^g = H$ for all $g \in G$.*

In order to better understand what this means, let us recall a few more concepts.

Definition 2.3 (homomorphism) *Suppose that G and H are groups and that $\phi : G \to H$ is a mapping from G to H. Then ϕ is called a homomorphism if $\phi(gh) = \phi(g)\phi(h)$ for all $g, h \in G$.*

Here are the names of particular types of homomorphisms. *Monomorphisms* and *epimorphisms* are the injective and surjective homomorphisms, respectively. *Isomorphisms* are the bijective homomorphisms. It can be shown that if ϕ is an isomorphism then the inverse mapping ϕ^{-1} (which exists since ϕ is bijective) is again a homomorphism, and hence an isomorphism. An *automorphism* of a group G is an isomorphim from G to itself.

What has this all to do with conjugation? The answer is in the following lemma.

Lemma 2.4 *The conjugation mapping c_g is an automorphism of G.* □

The conjugation automorphism c_g of G is said to be an *inner* automorphism of G, that is, it is constructed from G itself and from one of its elements.

One important property of homomorphisms is that they take subgroups to subgroups. Applying this to c_g, we see that if $H \leq G$ and $g \in G$ then $H^g \leq G$, *i.e.*, H^g is again a subgroup of G. The subgroup H^g is said to be *conjugate* with H in G. If we take at random a group G, a subgroup $H \leq G$ and an element $g \in G$ then we cannot expect, of course, that the subgroups H and H^g are equal. Thus, the normal subgroups, as defined above, are very special in that $H = H^g$ for all g if H is normal in G. The normal subgroups of H are the ones that are left invariant (not moved as a set, while the individual elements of H may move) under every conjugation automorphism (or we can now say, by every inner automorphism) of G.

For every group G the subgroups $\{1_G\}$ (the *trivial* subgroup) and G are normal in G. We say that the subgroup $G \leq G$ is *improper* in the sense that it is not smaller than G. All the other subgroups, that is, the subgroups $H \leq G$ with $H \neq G$ are called *proper*.

Definition 2.5 (simple group) *A group G is called simple if it has exactly two normal subgroup, i.e., the trivial subgroup and G itself.*

We can also restate this as follows: in a simple group none of the proper nontrivial subgroups is normal. So here is a question: Is the group of order one simple? (Recall that the *order* $|G|$ of the finite group G is the number

of elements in G; we will also sometimes call this number the *size* of G.) If G is of order one then $G = \{1_G\}$. Thus the group of order one has no proper nontrivial subgroups at all, so certainly none of "them" is normal. However, we don't want to call the group G of order one simple, and as the formal grounds for this we cite Definition 2.5, whereby a simple group must have exactly two normal subgroups. This fails for the group of order one, because it has only one subgroup!

On a less formal level, we don't want to call the group of order one simple for the same reason that we don't want to call the integer one a prime number. We use the prime numbers as building blocks of all integers. Every positive integer is a product of primes, so primes serve as *factors* of integers. Well, in this respect the number one is certainly a totally useless factor. Similarly for groups: we will see shortly that the finite simple groups are the building blocks of all finite groups, and the group of order one is a useless building block.

In the remainder of this section we attempt a little classification, namely, we classify all abelian simple groups. Recall that a group G is *abelian* if and only if all elements of G *commute*, that is, $gh = hg$ for all $g, h \in G$.

Theorem 2.6 *Every abelian simple group is (isomorphic to) a cyclic group $\mathbb{Z}_p$, where p is a prime.*

Note that we don't assume finiteness of the group—it is unnecessary.

The proof is a combination of two lemmas.

Lemma 2.7 *If G is an abelian simple group then G has no proper nontrivial subgroups, that is, the trivial subgroup $\{1_G\}$ and G itself are the only subgroups of G.*

Proof. Since G is abelian, $h^g = g^{-1}hg = g^{-1}gh = h$ for all $g, h \in G$, that is, every conjugation automorphism c_g sends every h to h. In particular, $H^g = \{h^g \mid h \in H\} = \{h \mid h \in H\} = H$ for all $H \leq G$. Thus, every subgroup of G is normal.

Since G is simple, Definition 2.5 yields that $\{1_G\}$ and G are the only subgroups of G. □

For the second lemma, we need a brief refresher on cyclic groups.

Suppose G is an arbitrary group. Recall that, for $g \in G$ and $n \in \mathbb{Z}$, we define the *power* g^n of g as follows:

$$g^n = \begin{cases} gg \cdots g \ (n \text{ times}), & \text{if } n > 0; \\ 1_G, & \text{if } n = 0; \\ g^{-1}g^{-1} \cdots g^{-1} \ (|n| \text{ times}), & \text{if } n < 0. \end{cases}$$

The notation for powers, g^n, is similar to our exponential notation for conjugation, h^g. To stress similarity, let's conjugate the other way around, g^h. In practice, this similarity doesn't cause a serious problem. The difference is, clearly, that n in g^n is an integer, while h in g^h is an element of the group G.

The powers of an element satisfy the usual algebraic rules, namely, for all $n, m \in \mathbb{Z}$, we have $g^{n+m} = g^n g^m$ and $g^{nm} = (g^n)^m$. These rules imply the following key result.

Proposition 2.8 *For an arbitrary group G and $g \in G$, the set $\{g^n \mid n \in \mathbb{Z}\}$ is a subgroup of G.* $\square$

The subgroup $\{g^n \mid n \in \mathbb{Z}\}$ of G is called the *cyclic subgroup* generated by g. It is denoted by $\langle g \rangle$.

Definition 2.9 (cyclic group) *The group G is called cyclic if $G = \langle g \rangle$ for some $g \in G$.*

Note that according to this definition the group of order one is cyclic. Indeed, if $G = \{1_G\}$ then $G = \langle 1_G \rangle$.

We now turn to the classification of cyclic groups. First, recall what the order of an element is.

Definition 2.10 (order of an element) *The order $|g|$ of an element $g \in G$ is the smallest positive integer n such that $g^n = 1_G$. If no such n exists then $|g|$ is set to be infinity.*

If $|g| = \infty$ then all powers of g are distinct and so the subgroup $\langle g \rangle$ is infinite. If $|g| = n$ is finite then, for $i, j \in \mathbb{Z}$, we have $g^i = g^j$ if and only if n divides $i - j$. This implies that the subgroup $\langle g \rangle$ has exactly n elements, namely, they are $g^0 = 1_G, g^1 = g, g^2, \ldots, g^{n-2}$, and $g^{n-1} = g^{-1}$. In particular, in all cases $|\langle g \rangle| = |g|$.

Compare this with the definition of the group $\mathbb{Z}_n$: Let n be a positive integer. For $i, j \in \mathbb{Z}$ define $i \sim j$ if and only if n divides $i - j$. Then $\sim$ is an equivalence relation on $\mathbb{Z}$. Let $\bar{i}$ denote the equivalence class containing $i \in \mathbb{Z}$. There are exactly n equivalence classes, namely, they are the classes $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$. These equivalence classes are the elements of the group $\mathbb{Z}_n$; the group operation on $\mathbb{Z}_n$ (addition) is defined by $\bar{i} + \bar{j} = \overline{i+j}$.

Proposition 2.11 *If G is cyclic and $g \in G$ is such that $G = \langle g \rangle$ then $G \cong \mathbb{Z}$ if $|g| = \infty$ and $G \cong \mathbb{Z}_n$ if $|g| = n < \infty$.* □

Here is how the isomorphism claimed in this proposition can be defined. When $|g|$ is infinite then the mapping $\phi : \mathbb{Z} \to G$ defined by $\phi : i \mapsto g^i$ is the desired isomorphism. If $|g| = n < \infty$ then we take, instead, the mapping $\bar{\phi} : \mathbb{Z}_n \to G$ defined by $\bar{\phi} : \bar{i} \mapsto g^i$.

Finally, we require information about the subgroups of $\mathbb{Z}$ and $\mathbb{Z}_n$.

Theorem 2.12 *The following hold.*

(a) *The mapping $m \mapsto \langle m \rangle$ is a bijection between all nonnegative integers and all subgroups of $\mathbb{Z}$. In particular, $\mathbb{Z}$ has infinitely many subgroups.*

(b) *If n is a positive integer, then the mapping $m \mapsto \langle \bar{m} \rangle$ is a bijection between all positive divisors of n and all subgroups of $\mathbb{Z}_n$. In particular, $\mathbb{Z}_n$ has no nontrivial proper subgroups if and only if $n = p$ is a prime, or $n = 1$.* □

In particular, part (b) tells us that the groups $\mathbb{Z}_p$, p a prime, are simple.

After this refresher, we are ready to complete the proof of Theorem 2.6. If G is again an abelian simple group then, by Lemma 2.7, G has no nontrivial proper subgroups.

Lemma 2.13 *If a group G has no proper nontrivial subgroups then either G has order one or G is isomorphic to $\mathbb{Z}_p$ for a prime p.*

Proof. If G has order one then the claim trivially holds.

Now assume that $G \neq \{1_G\}$. We first show that G is cyclic. Pick $g \in G$ such that $g \neq 1_G$. Consider the cyclic subgroup $H = \langle g \rangle$. Clearly, H is not the trivial subgroup, since $g \neq 1_G$. By the assumptions of the lemma, H must be improper, so $H = G$, implying that $G = \langle g \rangle$ is cyclic.

According to Proposition 2.11, this means that G is isomorphic to either $\mathbb{Z}$, or $\mathbb{Z}_n$ for some n. Let ϕ be that isomorphism and let H denote the target group $\mathbb{Z}$ or $\mathbb{Z}_n$, that is, ϕ maps G to H. Also, let $\mathcal{S}$ be the set of all subgroups of G and $\mathcal{T}$ be the set of all subgroups of H. Note that ϕ maps the subgroups of G onto the subgroups of H, that is, ϕ induces a mapping $\hat{\phi}$ from $\mathcal{S}$ to $\mathcal{T}$. Similarly, $\psi = \phi^{-1}$ induces a mapping $\hat{\psi}$ from $\mathcal{T}$ to $\mathcal{S}$. Clearly, $\hat{\phi}$ and $\hat{\psi}$ are inverses of each other, which means that they establish a bijection between $\mathcal{S}$ and $\mathcal{T}$. In particular, $\mathcal{S}$ and $\mathcal{T}$ have the same size, that is, G and H have the same number of subgroups.

Since G has no proper nontrivial subgroups, neither has H. Since H is either $\mathbb{Z}$, or $\mathbb{Z}_n$, Theorem 2.12 yields that $n = 1$ or $n = p$ is a prime. Hence H has order one, or $H = \mathbb{Z}_p$, and consequently, G has order one (if H has), or $G \cong H = \mathbb{Z}_p$. □

Lemmas 2.7 and 2.13 together imply Theorem 2.6, which completes our classification of abelian simple groups.

Two remarks are in order. First, in the second part of the proof of Lemma 2.13 we use a very general observation. Namely, isomorphic groups have isomorphic subgroup structures. In particular, isomorphic groups always have the same number of subgroups. The second remark concerns the way we stated our little classification result, Theorems 2.6 (see also Theorem 1.1). In the theorems of this sort, there is a tendency to say "is" in place of "is isomorphic to". That is, groups that are isomorphic are viewed as being the same. This is slang and it shouldn't be understood too literally. For example, if two subgroups of the same groups are isomorphic (say, conjugate subgroups H and H^g), we shouldn't jump to the conclusion that they are in fact the same subgroup.

3 Composition series, composition factors

In this section we aim at proving the Jordan-Hölder Theorem. It is this theorem we mean when we say that finite simple groups are the building blocks of all finite groups.

Definition 3.1 (subnormal series) *Let G be a group. A (finite) series of subgroups $H_0 \leq H_1 \ldots \leq H_k = G$ of G is called a subnormal series in G if $H_{i-1} \trianglelefteq H_i$ for $1 \leq i \leq k$.*

Here is a related concept and notation:

Definition 3.2 (subnormal subgroup) *A subgroup H of G is called subnormal and we write $H \lhd\lhd G$ if H is a member of a subnormal series in G.*

We will call a subnormal series $H_0 \leq H_1 \ldots \leq H_k = G$ *proper* if it contains no repetition, that is, if $H_{i-1} \neq H_i$ for all i. From every improper subnormal series can be made proper by removing the repetitions and leaving each distinct member just once.

Given two subnormal series, $H_0 \leq H_1 \ldots \leq H_k = G$ and $K_0 \leq K_1 \ldots \leq K_m = G$, of G, we say that the second series is a refinement of the first one if, for $0 \leq i \leq k$, we have $H_i = K_{s_i}$ for some $0 \leq s_0 < s_1 < s_2 < \ldots < s_k = m$. That is, we get the first series by dropping a few members of the second one (and we never drop the last member, G). We will, of course, mostly deal with proper subnormal series and nontrivial refinement (*i.e.*, where $m > k$). In this case we will say that the second series is denser than the first one.

Definition 3.3 (composition series) *Suppose G is a finite group. A composition series in G is a proper subnormal series that cannot be properly and nontrivially refined.*

That is, a composition series is a series into which it is impossible to insert a new member, not equal to any existing member.

The same definition can be given for arbitrary groups, however, for general infinite groups it makes little sense, because we cannot guarantee the existence of composition series. Clearly, for finite groups composition series always exist.

Suppose $H_0 \leq H_1 \leq \ldots \leq H_k = G$ is a composition series of G. We first note that $H_0 = 1$, that is, every composition series starts from the trivial subgroup. The reason for this is that if $H_0 \neq 1$ then we cab insert the trivial subgroup before H_0, thus refining the series. By definition, this is impossible, hence $H_0 = 1$.

Since $H_{i-1} \lhd H_i$ for $i = 1, \ldots, k$, we can consider the factor groups $F_i = H_i/H_{i-1}$. These factor groups will be called the *composition factors* of G relative to the composition series $1 = H_0 \leq H_1 \leq \ldots\ H_k = G$. The number k will be called that *composition length* of G, again relative to this composition series. Our goal in this section is the Jordan-Hölder Theorem that claims that both the composition length and the set of composition factors, taken up to isomorphism, are independent of the choice of the composition series, and so they are true invariants of the group G.

However, before we state and prove the Jordan-Hölder Theorem, we establish the following important fact.

Proposition 3.4 *Every composition factor is a simple group.*

In order to prove this, we will need to recall certain results on homomorphisms and factor groups. Suppose $\phi : G \to H$ is a homomorphism. As usual, for a subset $X \subseteq G$, we denote $\phi(X) = \{\phi(g) \,|\, g \in X\}$. Reversely, if $Y \subseteq H$, we let $\phi^{-1}(Y)$ denote $\{g \in G \,|\, \phi(g) \in Y\}$. We will call $\phi^{-1}(Y)$ the *full preimage* of Y. When $Y = \{y\}$ is a singleton, we write $\phi^{-1}(y)$ in place of $\phi^{-1}(\{y\}$. Note that ϕ^{-1} above is just a notation; in general, there is no inverse mapping for ϕ, unless ϕ happens to be an isomorphism.

Theorem 3.5 (correspondence theorem) *Suppose $\phi : G \to H$ is a surjective homomorphism and let $K = \mathrm{Ker}\phi$). Let $\mathcal{G} = \{T \leq G \,|\, K \leq T\}$ be the set of all subgroups of G containing K, and let $\mathcal{H}$ be the set of all subgroups of H. Then ϕ induces a bijection between $\mathcal{G}$ and cH, whose inverse is given by the above "mapping" ϕ^{-1}. Under this bijection, normal subgroups correspond again to normal subgroups.* □

Suppose now $H \trianglelefteq G$ and let $F = G/H$. Let π be the canonical surjective homomorphism $G \to F$ sending $g \in G$ to the coset gH. Notice that $H = \mathrm{Ker}\pi$. Therefore, Theorem 3.5 implies that π and π^{-1} provide a bijective correspondence between all overgroups of H in G and all subgroups of F, with normal overgroups of H in G corresponding to the normal subgroups of F.

We can now prove Proposition 3.4.

Proof. Suppose some composition factor F_i is not simple. Then F_i contains a proper nontrivial normal subgroup, say, R, Let π be the canonical homomorphism $H_i \to F_i$, and let $\hat{R} = \pi^{-1}(R)$. Clearly, $\hat{R} \leq H_i$, and note that $H_{i-1} \leq \hat{R}$, because $H_{i-1} = \mathrm{Ker}\pi$. Consider the series obtained by inserting $H_{i-\frac{1}{2}} = \hat{R}$ between H_{i-1} and H_i. Clearly, $H_{i-1} \trianglelefteq \hat{R}$, since $H_{i-1} \trianglelefteq H_i$ and $\hat{R} \leq H_i$. Also, $\hat{R} \trianglelefteq H_i$ by the Correspondence Theorem, since $R \trianglelefteq F_i$. That is the new series is a subnormal series. Furthermore, H_{i-1} is the full preimage of the trivial subgroup of F_i and H_i is the full preimage of the entire F_i. Hence, by the same Correspondence Theorem, $H_{i-1} \neq \hat{R} \neq H_i$, since R is both nontrivial and proper in F_i. This means that the new subnormal series

is proper, that is, it is a proper refinement of the initial composition series. This is a contradiction. □

Note that Proposition 3.4 also works in reverse. Namely, the following is true.

Proposition 3.6 *Suppose G is a finite group and $1 = H_0 \leq H_1 \leq \ldots \leq H_k = G$ is a subnormal series, such that each factor $F_i = H_i/H_{i-1}$ is a simple group. Then this series is a composition series.*

Now we turn to the key result of this section.

Theorem 3.7 (Jordan-Hölder) *Suppose G is a finite group and suppose $1 = H_0 \leq H_1 \leq \ldots \leq H_k = G$ and $1 = H'_0 \leq H'_1 \leq \ldots \leq H'_{k'} = G$ are two composition series in G. Then $k = k'$. Furthermore, there is a permutation σ of $\{1, 2, \ldots, k\}$, such that $F_i \cong F'_{\sigma(i)}$ for all i. Here $F_i = H_i/H_{i-1}$ and $F'_j = H'_j/H'_{j-1}$ are the composition factors of G relative to the corresponding composition series.* □

In view of this theorem we will speak simply of the composition length and the set of composition factors of G.

Example 3.8 *Suppose $G = \mathbb{Z}_{24}$. What are the composition length and composition factors of G? Consider the following series in G:*

$$\langle \bar{0} \rangle < \langle \bar{8} \rangle < \langle \bar{4} \rangle < \langle \bar{2} \rangle < \langle \bar{1} \rangle = G.$$

Clearly, $\langle \bar{0} \rangle$ is the trivial subgroup of G. The series above is, clearly, subnormal since G is abelian and every subgroup of G is normal. Also, the factors of the above series are $F_1 \cong \mathbb{Z}_3$ and $F_2 \cong F_3 \cong F_4 \cong \mathbb{Z}_2$, and they are all simple groups. By Proposition 3.6, our series is a composition series. Hence, the composition length of G is four, and the composition factors of G are $\mathbb{Z}_3$ once and $\mathbb{Z}_2$ three times.

Example 3.9 *Let $G = \mathrm{Sym}(4)$. Consider the series*

$$1 < \langle (1,2)(3,4) \rangle < V_4 < \mathrm{Alt}(4) < \mathrm{Sym}(4) = G.$$

Here $V_4 = \langle (1,2)(3,4), (1,3)(2,4) \rangle = \{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ is the Klein four-group. Note that V_4 and $\mathrm{Alt}(4)$ are normal in G, and

that $\langle (1,2)(3,4) \rangle$ *is normal in* V_4*, since* V_4 *is abelian. Thus, the above series is a subnormal series in* G*. Furthermore, the factors of this series are* $F_1 \cong F_2 \cong F_4 \cong \mathbb{Z}_2$ *and* $F_3 \cong \mathbb{Z}_3$*. So the series above is a composition series of* $\mathrm{Sym}(4)$*. Furthermore,* $\mathrm{Sym}(4)$ *has the same composition length and composition factors as* $\mathbb{Z}_{24}$*. Note that* $\mathrm{Sym}(4)$ *and* $\mathbb{Z}_{24}$ *are not isomorphic. Indeed,* $\mathbb{Z}_{24}$ *is abelian, whereas* $\mathrm{Sym}(4)$ *isn't.*

Example 3.10 *Let* $G = \mathrm{Sym}(n)$*,* $n \geq 5$*. Consider the series* $1 < \mathrm{Alt}(n) < \mathrm{Sym}(n)$*. Since* $\mathrm{Alt}(n) \lhd \mathrm{Sym}(n)$*, this series is subnormal. Its factors are* $F_1 = \mathrm{Alt}(n)$ *and* $F_2 \cong \mathbb{Z}_2$*. We will see below that* $\mathrm{Alt}(n)$ *is simple, when* $n \geq 5$*. This means, by Proposition 3.6, that our subnormal series is in fact a composition series of* G*, and so* G *has composition length two and composition factors* $\mathrm{Alt}(n)$ *and* $\mathbb{Z}(2)$*.*

In these examples we deal with individual groups. If we want to be able to work with the whole families of groups, we need a few useful gadgets. First of all, let's set up some notation. For a finite group G let $\ell(G)$ denote the composition length of G, and $\mathrm{cf}(G)$ the set of composition factors of G. Note that the composition factors in $\mathrm{cf}(G)$ are taken up to isomorphism and that the same factor can appear in this set several times. So $\mathrm{cf}(G)$ is a multiset, rather than a usual set. For multisets, the operation of summation substitutes the union operation. For example, if a multiset A consists of five apples and three plums and a set B consists of an apple, two plums, and an orange then $A + B$ consists of six apples, five plums, and one orange.

Proposition 3.11 *Suppose* G *is a finite group and* $H \trianglelefteq G$*. Let* $K = G/H$*. Then* $\ell(G) = \ell(H) + \ell(K)$ *and also* $\mathrm{cf}(G) = \mathrm{cf}(H) + \mathrm{cf}(K)$*.*

Proof. Suppose $1 = H_0 < H_1 < \ldots < H_k = H$ is a composition series in H and $\bar{1} = K_0 < K_1 < \ldots < K_m = K$ is a composition series in K. Let π be the canonical homomorphism from G onto K. Set $\hat{K}_i = \pi^{-1}(K_i)$, $i = 0, 1, \ldots, m$. Notice that $\hat{K}_0 = H = H_k$ and $\hat{K}_m = G$. Consider the series

$$1 = H_0 < H_1 < \ldots < H_k = H = \hat{K}_0 < \hat{K}_1 < \ldots < \hat{K}_m = G.$$

Observe that $\hat{K}_{i-1} \lhd \hat{K}_i$ and, furthermore, $\hat{K}_i/\hat{K}_{i-1} \cong K_i/K_{i-1}$. First of all, this means that the above series is a subnormal series. Secondly, the first k factors of this series the composition factors of H (hence they are simple groups), while the remaining m factors are the composition factors of

K (hence also simple. By Proposition 3.6, the series above is a composition series in G, and the claims follow. □

Applying induction, we get the following generalization.

Corollary 3.12 *Suppose G is a finite group and $1 = H_0 \leq H_1 \leq \ldots \leq H_k = G$ is an arbitrary subnormal series in G. Set $F_i = H_i/H_{i-1}$ for all $i > 0$. Then $\ell(G) = \ell(F_1) + \ldots + \ell(F_k)$ and $\mathrm{cf}(G) = \mathrm{cf}(F_1) + \ldots + \mathrm{cf}(F_k)$.* □

As an application of these ideas let's prove the following.

Proposition 3.13 *Suppose G is a finite group. Let $m = \ell(G)$ and suppose $\mathrm{cf}(G) = \{S_1, S_2, \ldots, S_m\}$. Then $|G| = |S_1| \cdot |S_2| \cdots |S_m|$.*

Proof. We argue by induction on m. If $m = 0$ then $G = 1$ and the claim trivially holds. Now consider an arbitrary $m > 0$. Choose a composition series $1 = H_0 < H_1 < \ldots < H_m = G$ in G. We may assume without loss of generality that the composition factor H_m/H_{m-1} is S_m. Set $H = H_{m-1}$ and note that $H \lhd G$. In particular, $|G| = |H| \cdot |G/H| = |H| \cdot |S_m|$. Furthermore, notice that $1 = H_0 < H_1 < \ldots < H_{m-1} = H$ is a composition series in H and hence $\mathrm{cf}(H) = \{S_1, \S_2, \ldots, S_{m-1}\}$. By induction, $|H| = |S_1| \cdot |S_2| \cdots |S_{m-1}|$. Putting everything together, we get $|G| = |H| \cdot |S_m| = |S_1| \cdot |S_2| \cdots |S_m|$. □

We can now determine the composition factors of all finite abelian groups.

Proposition 3.14 *Suppose G is an abelian group of order $n = p_1^{s_1} p_2^{s_2} \cdots p_m^{s_m}$, where $p_1, p_2, \ldots, p_m$ are primes. Then $\ell(G) = s_1 + s_2 + \ldots + s_m$ and $\mathrm{cf}(G)$ consists of s_1 copies of $\mathbb{Z}_{p_1}$, s_2 copies of $\mathbb{Z}_{p_2}$, etc..*

Proof. Consider a composition series in G, say, $1 = H_0 < H_1 < \ldots < H_k = G$. Since G is abelian, every factor $F_i = H_i/H_{i-1}$ is also abelian. Hence every composition factor F_i is an abelian simple group. By Theorem **??**, we have $F_i \cong \mathbb{Z}_{r_i}$ for some prime r_i. On the other hand, Proposition 3.13 yields $|G| = r_1 r_2 \cdots r_k$. Comparing this with the equality $|G| = n = p_1^{s_1} p_2^{s_2} \cdots p_m^{s_m}$, we obtain the claimed. □

We remark that the abelian groups are not the only groups that have only abelian (*i.e.*, prime cyclic) composition factors. (See Example 3.9.) In fact, all soluble (also called solvable) groups have this property.

We conclude this section by introducing the so-called structure notation for finite groups. If a group G has a subnormal series with factors

$F_1, F_2, \ldots, F_k$, we will say that G has the structure $F_1.F_2.\ldots.F_k$. (The factors should be in the same order as in the series.) For example, Sym(4) has the structure $V_4.\mathbb{Z}_3.\mathbb{Z}_2$ or $\mathbb{Z}_2.\mathbb{Z}_2.\mathbb{Z}_3.\mathbb{Z}_2$, if we take the entire composition series from Example 3.9.

There is a very convenient simplification of this notation. Namely, in place of $\mathbb{Z}_n$ in the structure expressions we will write simply n. So we can now write 2.2.3.2 for $Sym(4)$. Extending this idea, if $F_i \cong Z_n \times Z_n \times \ldots \times \mathbb{Z}_n$ (m factors) is *homocyclic* then we will write n^m for such a factor. For example, $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, so $2^2.3.2$ is a good structure representation of Sym(4). We will see other bits and pieces of the structure notation later.

4 Permutations, permutation groups, symmetric and alternating groups

Permutations. Symmetric group.

$\mathrm{Sym}(\Omega) \cong \mathrm{Sym}(\Omega')$ if $|\Omega| = |\Omega'|$.

So it suffices to consider $\Omega = \{1, 2, \ldots, n\}$, $\mathrm{Sym}(n)$

Order of $\mathrm{Sym}(n)$

Even and odd permutations. Alternating group.

Cycles, independent cycles. Cycle decomposition, cyclic notation, cyclic type.

What happens with the cycle decomposition under conjugation.

Conjugacy classes in $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$. Sizes of conjugacy classes

Examples: Alt(3) and Alt(4).

Example: Simplicity of Alt(5) via conjugacy classes.

Simplicity of $\mathrm{Alt}(n)$, $n \geq 5$.

5 Permutation actions

Definition: Action on a set, equivalence of actions

Action as a homomorphism, kernel of action, faithful actions.

Transitive and intransitive actions. Orbits, actions on subsets (defined only if the subset is a union of orbits, transitive only if the subset is a single orbit).

Orbit from one element, notation for orbits.

Cosets, action by shifts, action on an orbit is equivalent to the action on cosets. Stabilizers, stabilizers are conjugate.

Example: Subgroups act on the group. Orbits–cosets.

Example: action by shifts on elements; regular action.

Example: action by conjugation on elements, orbits—conjugacy classes. stabilizers–centralizers.

Example: action by conjugation on subgroups

Homework problem: action on subsets by shifts and by conjugation.

6 Restricted permutation actions

Automorphisms of combinatorial and geometric objects

General setup

Example: 4-cycle, general graphs, affine plane, projective plane

Example: a different sort of restriction ? (continuous action, monotonic action) No, the same!

Designs, Witt design $W(24)$. Existence and uniqueness.

Uniqueness–in what sense?

Existence–MOG.

Mathieu group M_{24}