Permutation Groups

by Hendrik Lenstra

Universiteit Leiden

Lecture Notes

Written by Joris Weimar and Joost Michielsen,
Universiteit Leiden

Contents

Preface

These are the lecture notes to the course Permutation Groups as given by Hendrik Lenstra in the fall of 2007 at the University of Utrecht as part of the national Mastermath program. As the course progresses new sections will be added. Please notify Joris Weimar (jweimar@math.leidenuniv.nl) of any error you find in this document, be it of typographical or mathematical nature.

Chapter 1

Lecture 1

1.1 Groups, actions, and solvability

We will start with some basic definitions and quickly work towards stating the main theorem that will be proved in this course.

1.1. Definition. A group G is called solvable if there exists a chain of subgroups

$$G = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_k = \{1\}$$

with $H_{i+1} = [H_i, H_i]$.

1.2. Example. The symmetric group S_n is a solvable group iff $n \leq 4$.

1.3. Example. Every finite abelian group is solvable.

A natural thing to consider is the action of a group on a set.

1.4. Definition. Let G be a group and X a set. An action (or left action, or permutation representation) of G on X is a map $G \times X \longrightarrow X$ given by $(\sigma, x) \mapsto \sigma \circ x$, such that two axioms are satisfied

- $1 \circ x = x$ for all $x \in X$;
- $(gh) \circ x = g \circ (h \circ x)$ for all $g, h \in G$ and $x \in X$.

There is another definition that is equivalent (you are asked to prove this equivalence in the exercises).

1.5. Definition. An action of G on X is a homomorphism $\phi : G \longrightarrow \mathrm{Sym}(X)$

1.6. Definition. An action $\phi : G \longrightarrow \mathrm{Sym}(X)$ is called faithful if ϕ is injective. Equivalently: $\forall \sigma \in G \backslash \{1\} : \exists x \in X : \sigma x \neq x$, or, $\ker \phi = \{1\}$.

1.7. Definition. Let G be a group acting on a set X. Let $x \in X$ be given, then we call $G_x = \{\sigma \in G : \sigma x = x\}$ the stabilizer of x. This is a subgroup of G. We call $Gx = \{\sigma x : \sigma \in G\}$ the orbit of x.

1.8. Remark. There is a one-to-one correspondence between G/G_x and Gx.

This already gives us an interesting but weak version of the main theorem (see theorem 1.19). Note that if we just take any group G, without requiring solvability, that acts faithfully on a finite set X (we also don't require it to be primitive), then G can be regarded as a subgroup of the symmetric group. Hence, we have $\#G \leq n!$ and even $\#G | n!$ due to the theorem of Lagrange. Here, we have no constant power, like in the main theorem. Rather, we have an exponential expression that grows faster than 2^n. Also, the requirement of faithfulness in the main theorem is neccesary since it says that there is no part of the group that is not seen. If this requirement of faithfulness wasn't there, it would be impossible to bound the number of elements of G.

1.9. Definition. An action is called trivial if all elements of the group act as the identity.

1.10. Definition. A G-set is a set X together with an action of G on X.

To be formal, a G-set is actually an ordered pair, with on one coordinate the set X and on the other the map ϕ. But in practice we will say that X is G-set and the action will be understood.

1.11. Definition. A G-map is a map $f : X \longrightarrow Y$ such that

$$\forall \sigma \in G : \forall x \in X : f(\sigma x) = \sigma f(x).$$

with X, Y two G-sets.

A lot of terminology easily carries over. For example, a G-isomorphism is a bijective G-map between two G-sets X, and Y, written as $X \cong_G Y$. We can also talk about $\mathrm{Aut}_G(X)$, the group of G-automorphisms. The H in $X \cong_G G/H$ is only uniquely determined if H is a normal subgroup in G.

1.12. Definition. Let G be a group and H a subgroup, then we define $G/H = \{\tau H : \tau \in G\}$ the coset space whose elements are called cosets.

1.13. Definition. An action is called transitive if

- $X \neq \emptyset$.
- $\forall x, y \in X : \exists\, \sigma \in G$ such that $\sigma x = y$.

For a given subgroup H, the cosets naturally form a transitive G-set. Conversely, every transitive set is G-isomorphic to a G-set of the form G/H. So in a sense we can say that transitive G-sets don't give more information than subgroups. In fact, they may give less information in the sense that different subgroups give rise to isomorphic G-sets. These different subgroup are uniquely determined up to conjugacy, so unique if and only if H is a normal subgroup.
This gives us an equivalent definition of transitivity (see the exercises):

1.14. Theorem. An action is transitive iff a subgroup $H \subset G$ exists such that $X \cong_G G/H$.

1.15. Definition. A maximal subgroup H is a subgroup $H \subsetneq G$ such that there is no subgroup J with $H \subsetneq J \subsetneq G$.

Notice that, unlike commutative rings, which due to Zorn's lemma always have a maximal ideal, groups do not always have a maximal subgroup. For example, it can be shown that the additive group of rational numbers $(\mathbb{Q}, +)$ has no maximal subgroups. However, if we take any finitely generated group, Zorn's lemma works again and we see that such groups do have maximal subgroups. Hence it is clear that for example all finite groups, except for the trivial group, will have maximal subgroups. We will be mostly working with finite groups.

We now give a definition of a primitive G-set. It is a special kind of transitive G-set, where we put a restriction on the subgroup H that we find in the equivalent formulation of definition 1.13.

1.16. Definition. A G-set X is primitive if there is a maximal subgroup $H \subset G$ with $X \cong_G G/H$.

1.17. Definition. A G-invariant equivalence relation is an equivalence relation such that

$$x \sim y \iff \sigma x \sim \sigma y$$

for all $\sigma \in G$.

1.18. Example. Let X be the 4 corners of the unit square in the plane and G the group of symmetries of this square consisting of 4 rotations and 4 reflections, the D_4. We call two elements equivalent if their distance is not equal to 1.

An equivalent formulation of saying a G-set X is primitive, is saying that X is transitive, has more than one element, and has no G-invariant equivalence relations except the two trivial ones. This will also be left as an exercise. We are now ready to state the main theorem that will be proved in this course.

1.19. Theorem. There exist $c_0, c_1 \in \mathbb{R}_{\geq 1}$ with the following property. Let G be a finite solvable group acting faithfully and primitively on a set X. Then $\#G \leq c_0 \cdot (\#X)^{(c_1)}$.

1.20. Example. For example, $c_0 = 1$, and $c_1 = 4$ will do.

We can already see that if G is finite and the action of G on X is primitive and hence transitive, that X will also be finite. The cardinality will be the index of some subgroup and hence it will divide the order of G. This is why we don't have to require X to be finite in the theorem. This will automatically be the case.

We now return to solvable groups, basically groups that are built up from abelian groups.

1.21. Theorem. Take any abelian group G acting transitively and faithfully on a set X, then the sets G and X are in bijective correspondence to each other.

We see then that the main theorem (1.19) lifts the previous theorem 1.21 from the abelian case to the solvable case. Unfortunately we can't just replace the word primitive by the word transitive in the main theorem. There exists a finite solvable group G acting faithfully and transitively on X with the property that $\#G = 2^{(\#X-1)}$ (see exercises). If it is just this one example, then we could just call it c_0, and then c_1 can be anything. But there is actually an infinite sequence of examples with this property.

1.2 Galois theory

Let K be a field. For convenience we will assume $\mathrm{char}(K) = 0$. Now let $f \in K[x]$ be an irreducibe polynomial in x with degree n. Take $\alpha_1, \ldots, \alpha_n \in \bar{K}$ to be the zeroes of f. We then have the following finite extensions: $K \subset K(\alpha_1) \subset \cdots \subset K(\alpha_1, \ldots, \alpha_n) = L$. We can then look at the group $G = \mathrm{Aut}_K(L)$, the group of automorphisms that are the identity on K. The fundamental theorem of Galois theory states that given a finite Galois extension (such as the example $L \supset K$ as given above), there is a one-to-one correspondence between the fields F satisfying $L \supset F \supset K$ and the subgroups of its Galois group G.

This correspondence between subgroups of the Galois group and the intermediate fields is also possible to formulate in terms of G-sets. Rather than looking at the subgroups of

G, we look at the corresponding transitive G-sets. For example, if two groups in G are conjugate, their corresponding intermediate fields are isomorphic. This exactly relates to the fact that the corresponding G-sets are also isomorphic if the two subgroups are conjugate. The advantadge of formulating the fundamental theorem of Galois theory in terms of G-sets instead of subgroups is that it does not only classify all the intermediate fields, but also all the K-homomorphisms between them.

A typical G-set of interest here, is the set $X = \{\alpha_1, \ldots, \alpha_n\}$ with α_i zeroes of our irreducible polynomial f. In this particular case, we have G acting transitively on X. In terms of the equivalent definition of definition 1.13, we have $X \cong_G G/H$ with $H = \mathrm{Gal}(L/K(\alpha))$.

Continuing with this dictionary we can state our theorem 1.19 entirely in Galois theoretic terms and get a theorem about fields. So what do we get? The statement that G is solvable is equivalent by one of the big theorems of Galois to the existence of an radical expression for α with $f(\alpha) = 0$ in K. One obvious practical computational question to ask is, given an f, how can I tell whether such a radical expression exists? The problem is, that when the degree of f grows, the size of the Galois group grows exponentially! This will not be the way to decide whether L is solvable. The set X is clearly transitive, because the polynomial f is irreducible (try to prove this). In this case the action is faithful because L is the Galois closure of K. In this context, primitive also has a clear interpretation. The G-set X is primitive if and only if H is a maximal subgroup of G. Firstly, this means that the degree of $K(\alpha)$ of K is greater than 1, and secondly, there are no proper intermediate fields. This is not a bad condition because, if there are intermediate fields, you can break up the extension until you can't do it anymore. You reduce the problem to the primitive case where our main theorem gives us some upper bound. Here, we see an example of a theorem from pure mathematics motivated by very concrete and applied circumstances.

Chapter 2

Lecture 2

2.1 Exact sequences

Normally, exact sequences are defined in the category of abelian groups but we will discuss it in a more general setting (so also for non-abelian groups).

2.1. Definition. Let A, B, and C groups. We say that the sequence

$$A \xrightarrow{f} B \xrightarrow{g} C$$

is exact (at B) if $\mathrm{im} f = \ker g$.

Note that the composed map gf is the trivial map, mapping every element of A to the unit element of C. We can also consider a longer sequence

$$A_0 \longrightarrow A_1 \longrightarrow \cdots \longrightarrow A_n$$

which we call exact if it is exact at all A_i for $i = 1, \ldots, n-1$. Unless specified otherwise, we will write the trivial group as 1.

2.2. Examples. The sequence

$$1 \xrightarrow{f} B \xrightarrow{g} C$$

is exact if and only if g is an injection (where f is the unique group homomorphism from 1 into B). The sequence

$$B \xrightarrow{f} C \longrightarrow 1$$

is exact if and only if f is surjective. And the sequence

$$1 \xrightarrow{f} B \xrightarrow{g} 1$$

is exact if and only if $B = 1$.

If we look at the sequence

$$1 \longrightarrow B \xrightarrow{f} C \longrightarrow 1,$$

we see that this gives us $B \xrightarrow[f]{\sim} C$. We can also regard

$$1 \longrightarrow B \xrightarrow{g} C \xrightarrow{h} D,$$

and view B as a subgroup of C through g since g is injective. We can then, understanding that we identify B with it's image, say that B 'is' the kernel of h. If we do the same thing in reverse, we have

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1. \tag{2.3}$$

In this example you can see why people like to talk about exact sequences in the context of abelian groups. We have that C is the surjective image of g. So C may be identified with B modulo some normal subgroup. The exact sequence gives us $f(A) \triangleleft B$ and hence $B/f(A)$ 'is' C (identified through g, since it is surjective). We can in fact only complete the exact sequence $A \longrightarrow B$ to an an exact sequence like (2.3) with g if $f(A)$ is a normal subgroup. This will of course be the case if we only regard abelian groups, which will happen when we will regard modules over rings later. We then call $B/f(A)$ the cokernel. An even longer sequence is

$$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1. \tag{2.4}$$

These are called short exact sequences. We consider A as a normal subgroup of B (identified with the image) and we can identify C in a natural way with B/A. If two of the groups A, B, and C are finite, the third one must also be finite. We then have $\#B = \#A \cdot \#C$. We again consider the sequence (2.4). We can often control the group B (such as the order, or structure), by studying the groups A and C. We also say that we have an extension of C by A. One can wonder, given two extensions of C by A, one with B, and the other with B' in the middle, whether B is isomorphic to B'. And we mean a special kind of group isomorphism here, one that makes the following diagram commute:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{\phi} & B & \xrightarrow{\psi} & C & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id_A}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}_C} & & \\ 1 & \longrightarrow & A & \xrightarrow{\Phi} & B' & \xrightarrow{\Psi} & C & \longrightarrow & 1. \end{array} \tag{2.5}$$

This means we want to have that $\Phi = f\phi$ and $\psi = \Psi f$. So, if we can find a group homomorphism f that makes this diagram commutes, we will call these two extensions

equivalent or isomorphic. Notice that we do not require f to be an isomorphism of groups since this is automatically the case (see exercises). Thus, when we view extensions, we will view them up to this notion of isomorphism which is clearly an equivalence relation. We can make a very natural exact sequence by considering the direct product of two groups:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{g} & A \times C & \xrightarrow{h} & C & \longrightarrow & 1 \\ & & & & (\alpha, \gamma) & \longmapsto & \gamma & & \\ & & & & \alpha & \longmapsto & (\alpha, 1). & & \end{array} \tag{2.6}$$

It is clear that this is a short exact sequence, and thus an extension of C by A. We have to be careful when talking about extensions of C by A since there are examples of isomorphic groups B and B' that both fit in a short exact sequence with A and C but are non-isomorphic short exact sequences. In these cases the isomorphisms do not satisfy the conditions that make the diagram (2.5) commute.

2.7. Example. Let A and C be groups of order 2. There are at least two extensions of C by A. Namely, $B = V_4$ and $B = C_4$ (see exercise 31).

2.8. Definition. Consider the short exact sequence (2.4). We call it a split exact sequence if there exists a homomorphism $h : B \longrightarrow A$ such that $hf = \mathrm{id}_A$. If there exists a homomorphism $h : C \longrightarrow B$ such that $hf = \mathrm{id}_C$ then we call the sequence a semi-split exact sequence. Furthermore, if the sequence is split, it will take the form of sequence (2.4).

What this definition of semi-split says, is that we require the section to lift an element of C to it's fiber in B. An equivalent way of looking at it, is the observation that the normal subgroup A of B has a complement, where a complement is a set of representatives $\{1, b_1, b_2, \dots\}$ for the cosets (the fibers) $\{A, b_1A, b_2A, \dots\}$ that forms a subgroup. This will be a subgroup of B that is isomorphic to C with one element in each coset of A in B. Since A is normal in B we do not need to distinguish between left or right cosets of A. Now if B is abelian, then semi-split is equivalent to split. The equivalence is actually also valid under weaker conditions, for example if A lies in the $Z(B)$, the center of B. This motivates the next section.

2.2 The semidirect product

We have seen that if the group B in (2.4) is not abelian, and if the sequence semi-splits, the sequence isn't necessarily isomorphic to the direct product of A and C. In the case that the exact sequence semi-splits, it will in fact be isomorphic to a semidirect product of A and B. We now give a definition.

2.9. Proposition. Given groups A and C and a group homomorphism $\phi : C \longrightarrow \mathrm{Aut}(A)$ we define an operation $\star_\phi$ or just $\star$ on the cartesian product of A and C:

$$(\alpha_1, \gamma_1) \star (\alpha_2, \gamma_2) = (\alpha_1 \phi(\gamma_1)(\alpha_2), \gamma_1\gamma_2).$$

The operation defines a group operation and the resulting group will be called the semidirect product, written as $A \rtimes_\phi C$ or just $A \rtimes C$ if ϕ is understood.

We will leave the verification of this to the reader. If we are given two groups A, and C, there is only one direct product. Namely, the cartesian product with component-wise operations. However, we see that there are many semidirect products. Unlike with direct products, we can not turn the semi-product around (swapping A and C). This, of course, follows directly from the definition. Also, note that if we choose ϕ in (2.9) to be the trivial map, we get the direct product.

We will see that this semidirect product tells us exactly what is happening in a semi-split sequence. We can regard $A \rtimes C$ as an extension of C by A. We will have that A is a normal subgroup of $A \rtimes C$. This gives some motivation for the $\rtimes$ symbol (compare to $\lhd$).

Now look at the sequence

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{g} & A \rtimes C & \xrightarrow{h} & C & \longrightarrow & 1 \\ & & & & (\alpha, \gamma) & \longmapsto & \gamma & & \\ & & \alpha & \longmapsto & (\alpha, 1). & & & & \end{array} \tag{2.10}$$

We can conclude that an equivalent way of saying that the short exact sequence (2.4) is semi-split, is saying that it is isomorphic (as an extension) to an extension of the form (2.10).
One can check that this sequence is exact. It is obviously semi-split since we can take the group homomorphism $f : \gamma \mapsto (1, \gamma)$ (check this statement) so that $hf = \mathrm{id}_C$. So we see that C is a subgroup of this semidirect product. Not that the projection from $A \rtimes C$ onto A will not be a group homomorphism unless ϕ is the trivial map.

We can view $\mathrm{Aut}(A)$ as contained in $\mathrm{Sym}(A)$, the symmetries of the underlying set of A. So if we're given a group homomorphism $\phi : C \longrightarrow \mathrm{Aut}(A)$ then in particular we're given a group homomorphism from C to $\mathrm{Sym}(A)$. This is to say that through ϕ, the group C acts on the underlying set of A. But of course we know more about this action. Each element of C acts through a group homomorphism (isomorphism actually):

$$\begin{array}{ccc} C \times A & \longrightarrow & A \\ (\gamma, \alpha) & \longmapsto & {}^\gamma\alpha = \phi(\gamma)(\alpha) \end{array} \tag{2.11}$$

However, we need one axiom to ensure that the image of ϕ does not just lie in the symmetric group but in fact the automorphism group. This axiom is that for any given γ, we have ${}^{\gamma}(\alpha\beta) = {}^{\gamma}\alpha \cdot {}^{\gamma}\beta$ for all $\alpha, \beta \in A$, so that the action is a group homomorphism. But since it was already a bijection, we conclude that it is in fact a group automorphism. This gives us the following definition (where G plays the role of our C).

2.12. Definition. Let G be a group. By a G-group (or G-module if A is abelian) we mean a group A equipped with an action $G \times A \longrightarrow A, (\sigma, \alpha) \mapsto {}^{\sigma}\alpha$, of G on the underlying set of A, such that for all $\sigma \in G, \alpha, \beta \in A$ one has ${}^{\sigma}(\alpha\beta) = {}^{\sigma}\alpha \cdot {}^{\sigma}\beta$; equivalently, it is a group homomorphism $\phi : G \longrightarrow \mathrm{Aut}(A)$, the connection between the two definitions being given by the formula ${}^{\sigma}\alpha = \phi(\sigma)(\alpha)$.

A surprising law of nature is, that when you encounter these G-groups, most of the time they will be abelian. And then they are not called G-groups, but G-modules. This gives rise to a funny situation, namely, that abelian groups are often written in an additive way, whereas G, which need not be abelian, is often written in a multiplicative way. This often means that when you talk about a semidirect product, you have difficulty picking the right type of notation for this group since it's put together from an additive group and a multiplicative group.

A short note on generators: for a group C and an C-group A we can describe the group $A \rtimes C$, in terms of generators and relations as follows: the generators are just $A \sqcup C$ (you could make it thinner by replacing A and C by subsets that generator them, but then you have to modify your relations). So we just take a letter for each element of the underlying sets of A and C. There are two types of relations. Namely, all group relations holding in A ($a \cdot b = c$), and the same for C. The second relation is that if we take $\alpha \in A, \gamma \in C$ then we have the relation $A \ni {}^{\gamma}\alpha = \gamma\alpha\gamma^{-1}$.

2.3 A step towards the main theorem

The semidirect product that we have just discussed comes up in the following theorem. This theorem deals directly with the subject of the main theorem (1.19).

2.13. Remark. The group $A \rtimes C$ acts on the underlying set of A (not on the group A) by $(\alpha, \gamma) \cdot \beta = \alpha^{\gamma}\beta$ with $\alpha, \beta \in A$ and $\gamma \in C$ (see exercise 34).

2.14. Definition. Let G be a group and N normal in G. We call N a minimal normal subgroup if it contains exactly two different normal subgroups, namely the trivial group and N itself.

2.15. Example. Every finite group not isomorphic to the trivial group has a minimal normal subgroup.

2.16. Definition. Let H be a group and let N be an H-module. We say that N is simple if N has exactly two sub-H-modules, the trivial one and N itself.

2.17. Definition. We call a group N elementary abelian if there is a prime p and a $k \in \mathbb{Z}_{\geq 0}$ such that $N \cong (\mathbb{Z}/p\mathbb{Z})^k$.

2.18. Theorem. Let G be a finite solvable group acting faithfully and primitively on a set X. Let $x \in X$, let $H = G_x$ be the stabilizer of x, and let N be a minimal normal subgroup of G. Then the following statements hold:

(a) N is the only minimal normal subgroup of G;

(b) N is elementary abelian and N is the only non-trivial abelian normal subgroup of G;

(c) the map $\phi : N \longrightarrow X, \mu \mapsto \mu x$ is a bijection;

(d) H is solvable, N is a faithful H-module through the action ${}^{\sigma}\mu = \sigma\mu\sigma^{-1}$ for $\sigma \in H$ and $\mu \in N$, and N is simple as an H-module;

(e) the map $\psi : N \rtimes H \longrightarrow G$, $(\mu, \sigma) \mapsto \mu\sigma$ is a group isomorphism;

(f) the action of G on X is derived through ψ and ϕ from the action of $N \rtimes H$ on N (as in 2.13):

$$\begin{array}{ccc} (N \rtimes H) \times N & \longrightarrow & N \\ \downarrow{\scriptstyle (\psi,\phi)} & & \downarrow{\scriptstyle \phi} \\ G \times X & \longrightarrow & X. \end{array}$$

Let it be noted that G cannot be the trivial group because it acts primitively on a set X. As we see in the theorem, the set X has the same cardinality as N, where $G \cong N \rtimes H$. The set X is going to be endowed with some extra structure by our normal subgroup N. This already gives some control on the bound for the order of G. Since we have $|X| = |N| = p^k$, we are left with determining the order of the subgroup H and have thus reduced the problem of the main theorem to determining an upper bound for the order of H.

Chapter 3

Lecture 3

3.1 Proof of Theorem 2.18

To be able to prove theorem 2.18, we will need two more lemmas:

3.1. Lemma. Let a group G act on a set X and let $M \lhd G$. Then the equivalence relation $\sim_M$ defined by $x \sim_M y \iff \exists \tau \in M : y = \tau x$ is G-invariant.

Proof Suppose $x \sim_M y$, then we know $y = \tau x$ for some $\tau \in M$. We see that for any $\sigma \in G$ we have $\sigma y = \sigma\tau x = \sigma\tau\sigma^{-1}(\sigma x)$. Because M is normal in G, we have $\sigma\tau\sigma^{-1} \in M$, so $\sigma x \sim_M \sigma y$ follows. This proves that $\sim_M$ is G-invariant. □

3.2. Lemma. Let G be a group, and N, M normal subgroups of G such that $N \cap M = \{1\}$. Then $\forall \sigma \in N, \tau \in M : \sigma\tau = \tau\sigma$ and $NM = \{\sigma\tau : \sigma \in N, \tau \in M\}$ is a normal subgroup of G isomorphic to $N \times M$.

Proof In order to prove the first statement, we take $\sigma \in N, \tau \in M$ arbitrary and look at the commutator $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$. Since both N and M are invariant under conjugation, we see that $\sigma\tau\sigma^{-1} \in M$ and $\tau^{-1} \in M$, so $[\sigma, \tau] \in M$, but also $\sigma \in N$ and $\tau\sigma^{-1}\tau^{-1} \in N$, so $[\sigma, \tau] \in M$. This means $[\sigma, \tau] \in N \cap M$, hence $[\sigma, \tau] = 1$. This proves the first statement. To prove that NM is normal in G, we only have to note that for any $\sigma \in G$ we have $\sigma NM\sigma^{-1} = \sigma N\sigma^{-1}M = NM$. Furthermore, the map $f : N \times M \to NM$ given by $f(n, m) = nm$ clearly induces an isomorphism, precisely because $nm = mn$ and $M \cap N = \{1\}$. □

Now we are ready to prove theorem 2.18.

Proof of 2.18 We let G, X, N, x, H_x be as stated in 2.18. We will start with proving (a), (b) and (c) sort of simultaneously. First note that N, as a subgroup of a solvable group, has to be solvable. This means that $[N, N] \subsetneq N$, so $[N, N] = \{1\}$ because $[N, N]$ is normal in G (exercise 4) together with minimality of N. Hence N must be abelian. Now let $M \lhd G$ be non-trivial and abelian. By lemma 3.1, we have either $u \sim_M v \iff u = v$ or $u \sim_M v$

for all $u, v \in X$, because G acts primitively on X. So these two cases we have to consider. The first case is impossible: this would mean $\forall \tau \in M, \forall u \in X : \tau u = u$, implying that each $\tau \in M$ acts on X as the identity, so $M = \{1\}$ by the faithfulness of the action.

The next thing we are going to prove is that, under these conditions, M has actually no stabilizers. Consider the following map:

$$\begin{array}{ccc} M & \longrightarrow & X \\ \tau & \longmapsto & \tau x \end{array}$$

(3.3)

Note that the x taken here is the x picked beforehand. This map has to be surjective, because we know that for every $u \in X$ there is an $\sigma \in M$ such that $\sigma x = u$. Furthermore, for any $y \in X$ we have, taking $y = \tau x$, $M_y = M_{\tau x} = \tau M_x \tau^{-1} = M_x$, because M is abelian. So any $\tau \in M_x \subset G$ acts as the identity on X. Because the action of G on X was faithful, we can conclude $M_x = \{1\}$. Altogether, by 1.8 , we can conclude that the map is a bijection.

We proved: any non-trivial abelian normal subgroup M of G satisfies $\#M = \#X$. Because N was also abelian, this means $\#M = \#N$. Because N was minimal in G, we see that $N \cap M$ is either $\{1\}$ or N. If the latter is true, we are done. But the first certainly isn't true, since by lemma 3.2 the group MN with cardinality $(\#X)^2 > \#X$ would be both abelian and normal, which is a contradiction. Now we have proved (a), because any minimal normal subgroup of a solvable group is abelian. We have also proved (c): in fact we already gave the bijection (since M is equal to N). To prove (b) entirely, we need to show that N has to be elementary abelian, so of the form $(\mathbb{Z}/p\mathbb{Z})^k$ for some k and prime p. To prove this, we pick an element $y \in N$ of prime order, let's say the order of y is p. Now consider the subgroup $N[p] = \{z \in N : z^p = 1\} \subset N$. We see that $\forall \sigma \in G, \forall z \in N[p] : (\sigma z \sigma^{-1})^p = \sigma z^p \sigma^{-1} = 1$, so $N[p]$ will be normal and non-trivial in G, so $N[p] = N$. Since $N[p]$ is clearly elementary abelian, we are done.

Now we will continue to prove (d), (e) and (f). We have the following N-isomorphisms:

$$\begin{array}{ccccc} G/H & \xrightarrow{\sim} & X & \longleftarrow & N \\ \sigma H & \longmapsto & \sigma x & & \\ & & \tau x & \longleftarrow\!\shortmid & \tau \end{array}$$

We see that the map $N \to G/H$ given by $\tau \mapsto \tau H$ also has to be a bijection (but not necessarily a group isomorphism, H does not have to be normal in G). Hence, the map $N \rtimes H \xrightarrow{\psi} G$ given by $(\mu, \sigma) \mapsto \mu\sigma$ is a bijection. If we can show that the map is also a group homomorphism, we have proved (e). This is a straightforward computation: Let $\mu, \nu \in N; \sigma, \tau \in H$. Then we have $\psi(\mu, \sigma)\psi(\nu, \tau) = \mu\sigma \cdot \nu\tau = \mu\sigma\nu\sigma^{-1} \cdot \sigma\tau = \psi(\mu^\sigma \nu, \sigma\tau) =$

$\psi((\mu,\sigma)(\nu,\tau))$. This proves (e), now we continue to prove (f). To do this, we must prove that the following diagram is commutative:

$$\begin{array}{ccc} (N \rtimes H) \times N & \longrightarrow & N \\ \downarrow{\scriptstyle (\psi,\phi)} & & \downarrow{\scriptstyle \phi} \\ G \times X & \longrightarrow & X. \end{array}$$

Let $((\nu,\tau),\mu) \in (N \rtimes H) \times N$. If we go from $(N \rtimes H) \times N$ to N first, then $((\nu,\tau),\mu)$ will be first be mapped to $\nu^\tau\mu = \nu\tau\mu\tau^{-1}$, and then to $\nu\tau\mu\tau^{-1}x = \nu\tau\mu x$ because τ is in the stabilizer of x. If we go from $(N \rtimes H) \times N$ to $G \times X$, then $((\nu,\tau),\mu)$ will be mapped to $(\nu\tau, \mu x)$ first, and then to $\nu\tau\mu x$. So the diagram is indeed commutative, and (f) has been proved.

Now the only thing left to do is proving (d). To see that N is a faithful H-module under the action ${}^\tau\mu = \tau\mu\tau^{-1}$ with $\tau \in H, \mu \in N$, we use the diagram to see that $N \cong X$ as an H-set. Clearly, H acts faithfully on X, so H also has to act on N faithfully. N is even a simple H-module: for any sub H-module $M \subset N$, the normalizer $\mathcal{N}_G(M) = \{\sigma \in G : \sigma M \sigma^{-1} = M\}$ of M in G contains both H (because M is an H-module) and N (because N is abelian). Therefore it has to be equal to G by (e). From this follows that M is normal in G, so $M = \{1\}$ or $M = N$. This concludes the proof of theorem 2.18.

3.2 Consequences of the theorem

A direct consequence of this theorem, as was already stated in the previous chapter, is that $|X| = |N| = p^n$ for some prime p. Conversely, for every prime power it is possible to construct a group and a set satisfying all the relevant conditions. The theorem also provides us with a way to prove a well known statement from field theory.

3.4. Theorem. Let k be a finite field. Then k has order p^d for some prime p and some integer d.

Proof We know $k^+ \rtimes k^* \rtimes \mathrm{Aut}(k)$ is a solvable group acting primitively and faithfully on k from exercise 24, which was also shown in class. An immediate consequence of theorem 2.18 is that $|k|$ has to be p^d for some prime p and some integer d. □

Another consequence is that, when given an action $G \circlearrowright X$, it will be more or less sufficient to look at the action $H \circlearrowright N$. To make this exact, we will need some additional hypothesis, as well as some algebra outside group theory. In a few lectures we will be completely ready for this. Now, however, we will give an outline of the advantages of the new situation. For example, N is not just a stupid set anymore, it is a vector space. By this means we can reformulate our problem in terms of linear representations. Note that, exactly because N is a vector space, $\mathrm{Aut}(N) \cong \mathrm{GL}(d, \mathbb{F}_p)$. So making N into an H-module is the same (when a basis has been chosen) as giving a group homomorphism $H \hookrightarrow \mathrm{GL}(d, \mathbb{F}_p)$. So N

is a d-dimensional representation of the group H. The faithfulness of the action means that the homomorphism will be injective, and the simplicity of N means, in terms of linear representations, that the representation is irreducible.

Chapter 4

Lecture 4

4.1 Modules

We will start with a definition.

4.1. Definition. Let R be a ring. An R-module is an abelian group M (additively written) together with a map $R \times M \to M, (r, x) \mapsto rx$ such that for any $r, s \in R, m, n \in M$:

1 $(r + s)m = rm + sm$

2 $r(m + n) = rm + rn$

3 $(rs)m = r(sm)$

4 $1m = m$

Common choices for R are $R = \mathbb{Z}$ (then any abelian group is an R-module, $R = k$ with k some field (then the R-modules are the vector spaces) or $R = \mathbb{Z}[G]$, the group ring of G over $\mathbb{Z}$ (see definition 4.2). We will be using the last one a lot in the lectures to come.

Just as an equivalent way of describing an action G on a set X is through a group homomorphism $\phi : G \longrightarrow \mathrm{Sym}(X)$, an equivalent way of stating definition is saying that an R-module is an abelian group M plus a ring homomorphism $\phi : R \longrightarrow \mathrm{End}(M)$ where $\mathrm{End}(M)$ is to be understood as $\mathrm{Hom}(M, M)$. If we write rm for $\phi(r)(m)$ then all the above properties can be easily derived from the axioms that the ring homomorphism ϕ satisfies.

4.2. Definition. Let R be a commutative ring and G a group written multiplicatively. We define the group ring $R[G]$ to be the set of all finite sums

$$\sum_{\sigma \in G} a_\sigma \sigma.$$

That is to say, almost all $a_\sigma \in R$ are the zero element of R. Addition is defined as

$$\sum_{\sigma\in G} a_\sigma\sigma + \sum_{\sigma\in G} b_\sigma\sigma = \sum_{\sigma\in G}(a_\sigma + b_\sigma)\sigma.$$

and multiplication as

$$\sum_{\sigma\in G} a_\sigma\sigma \cdot \sum_{\sigma\in G} b_\sigma\sigma = \sum_{\sigma\in G,\tau\mu=\sigma} (a_\tau b_\mu)\sigma.$$

We do not assume that our ring is commutative. In fact, we will be working with group rings $R[G]$ that are surely not commutative if G is not. A $\mathbb{Z}[G]$-module is in fact the very same notion as a G-module. We can view a G-module as an abelian group M together with an action given by a group homomorphism $\phi : G \longrightarrow \mathrm{Aut}(M) = (\mathrm{End}(M))^*$. Now if we want to map $\mathbb{Z}[G]$ to $\mathrm{End}(M)$ by means of a ring homomorphism (such that we get an $\mathbb{Z}[G]$-module), then that is equivalent to giving a group homomorphism between G and the ring $\mathrm{End}(M)^*$. This $Z[G]$-module gives us a lot of interesting properties that will encounter later. For example, $\mathbb{Z}[G]$ has an interesting ideal structure.

We have thus spoken of R-modules. There is however a distiction between left R-modules and right R-modules. What we have called R-modules are in fact left R-modules. A right R-module is an R^{opp}-module. Hence, the third axiom of definition 4.1 becomes $(ms)r = m(sr)$. Another type of multiplicative notation that one encounters frequently is ${}^r m$ (rm additive) for a left R-module and m^r for a right R-module. For example, the first axiom in definition 4.1 for a multiplicatively written right R-module takes the familiar form $m^{r+s} = m^r \cdot m^s$. Notice that when R is commutative, we have $R = R^{\mathrm{opp}}$ and there is no difference between left R-modules and right R-modules.

4.3. Definition. Let R, S be rings. An R-S-bimodule is an abelian group M with a left R-module structure and a right S-module structure such that one additional axiom is satisfied :

- $\forall r \in R : \forall m \in M : \forall s \in S : r(ms) = (rm)s$.

4.4. Examples.

- The ring R is a R-R-bimodule;
- a $\mathbb{Z}$-R-bimodule is simply a right R-module;
- or as we expect, an R-$\mathbb{Z}$-bimodule is simply a left R-module;
- and a $\mathbb{Z}$-$\mathbb{Z}$-bimodule is just an abelian group.

We will actually soon see that R-S-modules are exactly the same as $R \otimes_{\mathbb{Z}} S^{\text{opp}}$-modules. This statement will get more meaning in section 4.2 where we will discuss tensor products. Let's take a look at the morphisms between R-modules.

4.5. Definition. Let R be a ring, and M, N two R-modules. then we call a group homomorphism $f : M \longrightarrow N$ an R-homomorphism, also R-linear map, if

$$\forall r \in R : \forall m \in M : f(rm) = r \cdot f(m).$$

We denote the set of all R-linear maps between the R-modules M and N by ${}_R\mathrm{Hom}(M, N)$ (the R to the left indicates that we are in fact talking about left R-modules. This is in fact an abelian group under pointwise addition. If R is a commutative ring, then ${}_R\mathrm{Hom}(M, N)$ is an R-module. Let S, and T be a rings and suppose that our R-module M is an R-S-bimodule and that our R-module N is an R-T-bimodule, then ${}_R\mathrm{Hom}({}_RM_S, {}_RM_T)$ is in fact an S-T-bimodule.

We can also look at sub-R-modules.

4.6. Definition. Let R be a ring and M an R-module. We call N a sub-R-module if N is a subgroup of M and we have

$$\forall r \in R : \forall m \in N : rm \in N.$$

4.7. Examples.

- A sub-R-module of R is a left ideal;
- a sub-R-R-bimodule (definition is evident) is a two-sided ideal.

If you have a sub-R-module N of M, then M/N gets a natural sub-R-module structure where the canonical homomorphism $f : M \longrightarrow M/N$ is in fact an R-linear map. Thus we can talk about modules modulo sub-modules, about kernels, cokernels. This means that we can easily talk about R-modules in the context of exact sequences. In the case of exact sequences of groups, we saw that when the group is abelian, the exact sequence takes an especially nice form. And this is also the case with R-modules, since they are per definition also abelian groups. For any two R-modules M, and N and an R-linear map f between them, we have the following exact sequence:

$$0 \longrightarrow \ker f \longrightarrow M \xrightarrow{f} N \longrightarrow N/f(M) = \operatorname{coker} f \longrightarrow 0.$$

There are several operations that we can perform on R-modules. We will look at some of them. Let R be a ring and M, and N two R-modules. Consider the direct product $M \times N$. This is very naturally an R-module through the component-wise multiplication $r \cdot (m, n) = (rm, rn)$. The axioms in definition 4.1 are trivially satisfied. This product $M \times N$ is equivalent to the direct sum $M \oplus N$. However, matters become different, when we consider infinite products of R-modules. Let I be an index set and let M_i be an R-modules for each i and consider the product R-module:

$$\prod_{i \in I} M_i = \{(x_i)_{i \in I} : x_i \in M_i\}.$$

This is an R-module (that it is an abelian group is clear) by working component-wise: $r(x_i)_{i \in I} = (rx_i)_{i \in I}$. But for the direct sum we get:

$$\bigoplus_{i \in I} M_i = \{(x_i)_{i \in I} \in \prod_{i \in I} : \#\{i \in I : x_i \neq 0\} < \infty\}.$$

We see that every M_i is embedded as a sub-R-module in the direct product by just taking all other components to be zero. Therefore, M_i is also embedded as a sub-R-module in the direct sum since there is only one component non-zero and 1 is certainly finite. The direct sum also has an interesting arrow-theoretic property. Namely, if we want to give an R-linear map between a direct sum of R-modules M_i and another R-module N, then it is necessary and sufficient to give R-linear maps from each M_i to N. For our purposes we will be most interested in the direct sum. A situation in which we will be finding ourselves soon, is that where the components of the direct sum are copies of the ring itself.

4.8. Definition. Let R be a ring. An R-module F is called free if there exists a set I such that

$$F \cong \bigoplus_{i \in I} R = R^{(I)} \subset R^I = \prod_{i \in I} R.$$

4.9. Examples.

- If R is a field, then an R-module is a vector space. The basis of this vector space (which by Zorn's lemma exists) tells us that such a set I exists. Hence, every module over a field is free.
- If we take $M = \mathbb{Z}/2\mathbb{Z}$ and $R = \mathbb{Z}$ then M is not a free module since a free $\mathbb{Z}$-module has no elements of finite order.

4.10. Definition. Let R be a ring and let M be an R-module. We say that M is simple if M has exactly two sub-R-modules, the zero module and M itself.

4.11. Theorem. Let R a ring and I a left ideal then R/I is simple (as an R-module) if and only if I is a maximal left ideal.

Proof. There exists a one-to-one correspondence between the sub-R-modules J of R that contain I and the sub-R-modules of R/I. Namely, J corresponds to J/I. The module R/I is simple if and only if it has exatly two sub-R-modules if and only if there are no sub-R-modules between I and R if and only if J is a maximal left ideal. □

What is more surprising is that there are no other simple modules. Regard the following theorem.

4.12. Theorem. Let R be a ring and M an R-module then the following holds: M is simple $\iff$ there exists a maximal left ideal $I \subset R$ such that $M \cong_R R/I$.

Proof. "$\Longleftarrow$": If there exists a maximal left ideal $I \subset R$ such that $M \cong_R R/I$ then theorem 4.11 tells us that M is simple since it is isomorphic to a simple module.

"$\Longrightarrow$": Pick an element $x \in M$ with $x \neq 0$ (this is possible because the zero-module is not simple. Now look at the map

$$\begin{array}{rccc} \phi: & R & \longrightarrow & M \\ & r & \longmapsto & rx. \end{array}$$

The mapping ϕ is R-linear and the image is $Rx = \{rx : r \in R\}$ which is not the zero-module since $x \neq 0$ and so $Rx = M$ since M is simple. Hence we can invoke the module-analogue of one of the isomorphism theorems and get $M \cong_R R/\ker\phi$. This kernel is a sub-module so it is a left ideal. But it is not just any left ideal. If we divide M out by this left ideal, we get a simple module. So the left ideal must be maximal. □

The situation of a simple R-module M is particularly nice when the ring R is commutative. In such a ring a maximal left ideal will automatically be two-sided. If we mod out our commutative ring R by this two-sided maximal ideal we get a field R/I. This means that M becomes a one-dimensional vector space over this field. Also, in the commutative case, it turns out that this maximal ideal I is uniquely determined by M (see exercises). If the ring is not commutative, such conclusions cannot be drawn.

4.13. Example. The abelian group $M = \mathbb{Z}/p\mathbb{Z}$ for p prime, is a simple $\mathbb{Z}$-module.

4.2 The tensor product

4.14. Definition. Let R be a ring, let A be a right R-module, let B be an R-module, and let C be an abelian group. We call a map $f : A \times B \longrightarrow C$ R-bilinear if the following three axioms are satisfied:

(i) for any fixed $a \in A$ we have $f(a, b + b') = f(a, b) + f(a, b')$ for all b, $b' \in B$;

(ii) for any fixed $b \in B$ we have $f(a + a', b) = f(a, b) + f(a', b)$ for all a, $a' \in A$;

(iii) $f(ar, b) = f(a, rb)$ for all $a \in A$, $b \in B$, and $r \in R$.

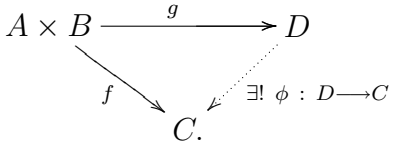
We will refer the set of all R-bilinear maps as $\mathrm{Bil}_R(A, B, C)$.

4.15. Definition. A tensor product of a right-R-module A and an R-module B over R is a pair (D, g) where D is an abelian group and $g \in \mathrm{Bil}_R(A, B, D)$ with the property that for all abelian groups C the map

$$\begin{array}{ll} \mathrm{Hom}(D, C) & \longrightarrow \mathrm{Bil}_R(A, B, C) \\ \phi & \longmapsto \phi \circ g \end{array}$$

is bijective.

This is to say that if we have a R-bilinear map g and someone gives us an abelian group C and another R-bilinear map f that there exists a unique group homomorphism ϕ such that the diagram below commutes:

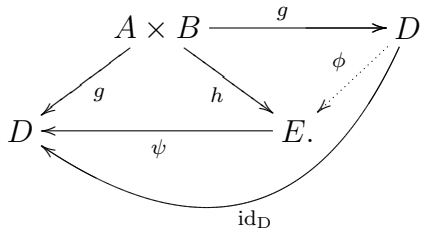


4.16. Example. If the tensor product exists, it will be commutative (in the sense that A tensored with B is isomorphic to B tensored with A).

In the theory of categories one would say that g satisfies the universal property. What we will see is that such a tensor product exists and that is basically unique. First, let us deal with uniqueness.

4.17. Theorem. Let R be a ring, let A be a right R-module, let B be an R-module, and assume that (D, g), and (E, h) are two tensor products of A and B over R then there exists a unique group isomorphism $\phi : D \longrightarrow E$ such that $\phi g = h$.

Proof. This is best proved by categorical reasoning (see diagram above). We are already given the unique group homomorphism ϕ such that the right triangle commutes. By definition of the tensor product we are also given a unique group homomorphism ψ such that the left triangle commutes. The claim is that ψ is actually the inverse of ϕ. In fact, one can easily check that the whole diagram commutes. It is obvious that the triangle $A \times B$, D, and D with the mappings g, g, and id_D commutes. Since this group homomorphism is unique, we must conclude that $\phi\psi = \mathrm{id}_D$. By a similar argument one shows that $\psi\phi = \mathrm{id}_D$.

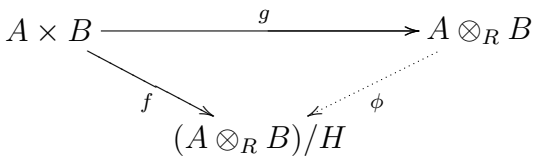


□

We will show the existence of the tensor product shortly. However, let us first look at, if they exists, how their are built up.

4.18. Theorem. The tensor product (D, g) of B and A over R, also written $A \otimes_R B$, is generated by the tensors $\{a \otimes_R b : a \in A, b \in B\}$ where $a \otimes_R b = g(a, b)$.

Proof. Take H to be the subgroup of D generated by $\{a \otimes_R b : a \in A, b \in B\}$. We have to show that $H = D$. Now look at the following diagram:



where ϕ is the canonical map and $g\phi$ is a R-bilinear map. We observe that the map f is in fact the zero map since the image of g ends up in the kernel of ϕ. Therefore, we can view the zero map as the composition of g with ϕ, but also as the composition of g with the zero map from the tensor product to the quotient. By uniqueness, we conclude that ϕ and the zero map are one and the same. This proves that $H = D = A \otimes_R B$. □

It is a common mistake to think that the tensor product is equal to the image of g (of all tensors). This would be clearly be the case if the image of g is a subgroup clearly. The image of a homomorphism is always a subgroup but the image of a bilinear map is not in general.

4.19. Example. (Assuming it exists) Take the tensor product $V_4 \otimes_{\mathbb{Z}} V_4$. The number of elements in the tensor product is 16 whereas the number of tensors is only 10. The other 6 elements are the sums of two such pure tensors.

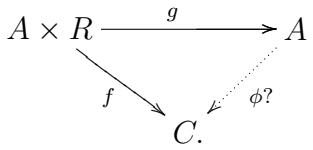
We will now show the existence of the tensor product. There are many different constructions of the tensor product (which are of course isomorphic up to a unique isomorphism). The one that will be exhibited here is not the shortest but has the advantage that it will give us some tools along the way to actually compute tensor products when confronted with them.

4.2.1 Fact 1

Let R be a ring and let A be a right R-module. Look at the map $g : A \times R \longrightarrow A$ defined by $(a, r) \mapsto ar$. The map g is clearly is R-bilinear. The claim is that (A, g) is a tensor product $A \otimes_R R$, so $A \otimes_R R \cong_R A$. In some way, if you view tensoring as multiplying modules together, then R acts as a unit element: it can be cancelled away. This R in place of B actually makes sense because R is a left-R-module.

4.20. Theorem. The pair (A, g) as defined above is a tensor product.

Proof. Look at the following diagram:



How should we define ϕ? We know that we should have that $\phi(ar) = f(a, r)$. So let's first define the map for $r = 1$. We should at least have $\phi(a) = f(a, 1)$. One can easily check that this ϕ is an R-linear map. We now verify that $\phi(ar) = f(ar, 1) = f(a, r \cdot 1) = f(a, r)$. □

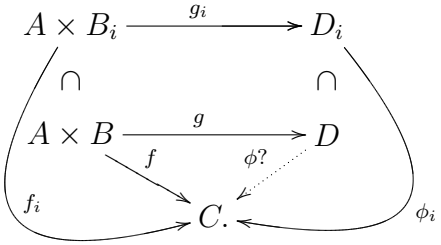
4.2.2 Fact 2

4.21. Theorem. Let $(B_i)_{i \in I}$ be a collection of left R-modules, suppose that $B = \bigoplus_{i \in I} B_i$ and let (D_i, g_i) be tensor products of A and B_i over R. Now define $D = \bigoplus_{i \in I} D_i$ and

$$\begin{array}{ll} g : A \times B & \longrightarrow D \\ (a, (b_i)_{i \in I}) & \longmapsto (g_i(a, b_i))_i \end{array}$$

then (D, g) is the tensor product $A \otimes_R B$.

Proof. The proof is very similiar to that of the first fact. Suppose that $f : A \times B \longrightarrow C$ is a bilinear map. Let's look at a diagram again (for a fixed $i \in I$):



The inclusions can be viewed as injective group homomorphisms. So we want to find a group homomorphism ϕ such that the triangle $A \times B$, D, C commutes. We now use the fact that the D_i are tensor products. One can easily check that the map f_i, which is the composition of the inclusion with f, is an R-bilinear map for each i. This means there exists a unique group homomorphism ϕ_i such that the outer 'triangle' commutes. As we have seen before, if we want to define a group homomorphism on a direct sum D, this is equivalent to giving a group homomorphism on each of the D_i. Let us take an element $x = (x_i)_{i \in I} \in D$ and define

$$\phi(x) = \sum_{i \in I} \phi_i(x_i)$$

(this is a finite sum since almost all x_i are zero). To show that ϕ works, we first note that ϕ is a group homomorphism. It remains to show that the lower triangle commutes. We want to have $\phi g = f$. But these are equal on the image of $A \times B_i$. Fix an element of A, and note that the B_i generate B and that ϕg and f are both group homomorphisms on B. If ϕg and f coincide on a set of generators, then they are equal. As for uniqueness of ϕ, if there is a different ϕ, say ϕ', that satisfies, then for a certain i the map ϕ'_i will be different from ϕ_i. But the ϕ_i were all unique by assumption. Hence, ϕ is uniquely defined. □

If we now combine Fact 1, that tells us that $A \otimes_R R$ exists, with the fact just acquired, we find that $A \otimes_R (\bigoplus_{i \in I} R) = \bigoplus_{i \in I} A$. So this means that we can take tensor products with free R-modules. Thus, in the case that R is a field we already know that tensor products exists.

We can rephrase the statement in theorem 4.21 as follows:

$$A \otimes_R \left(\bigoplus_{i \in I} B_i \right) \cong \bigoplus_{i \in I} (A \otimes B_i) .$$

If we consider the tensor product as an operation for multplying modules, and the direct sum as an operation for adding modules, we have found some sort of distributive law here.

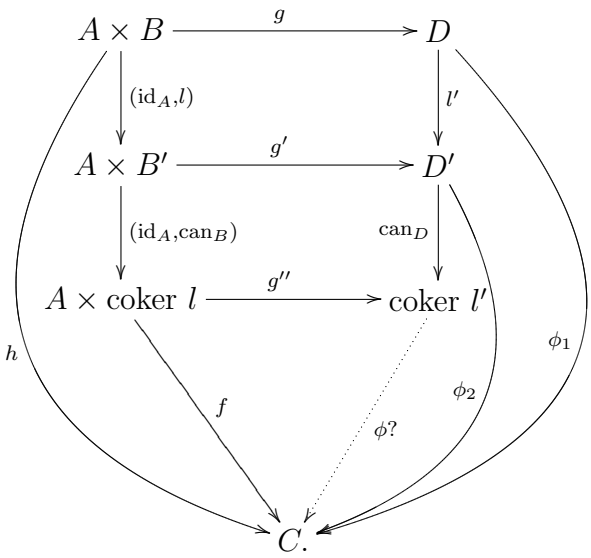
4.2.3 Fact 3

Let R be a ring, let A be a right R-module, and let B, and B' be two left R-modules. Let l be an R-linear map from B to B' and suppose that (D, g) and (D', g') are the tensor

products $A \otimes_R B$, and $A \otimes_R B'$ respectively. Then the claim is that we also have a tensor product $A \otimes_R \operatorname{coker} l$ where $\operatorname{coker} l = B'/l(B)$. Because the composition of (id_A, l) and g' is an R-bilinear map, we are given a unique group homomorphism $l' : D \longrightarrow D'$ with the property that it makes the top square in the diagram below commute.

We denote the canonical mapping of B' onto $B'/l(B)$ by can_B and the canonical mapping of D' onto $D'/l'(D)$ by can_D. We let $g'' : A \times \operatorname{coker} l \longrightarrow \operatorname{coker} l$ be the R-bilinear mapping that is induced by g'. Namely, the mapping is given by lifting an element from $A \times \operatorname{coker} l$ to $A \times B'$ and then applying $\mathrm{can}_D \circ g'$. One can easily check that this mapping is well-defined. This give us that $\mathrm{can}\, D' \circ g' = g'' \circ (\mathrm{id}_A, \mathrm{can})$. Now the big claim is, that if the top two lines in the diagram below are tensor products, then the bottom line is also.

4.22. Theorem. If (D, g) and (D', g') are tensor products $A \otimes_R B$, and $A \otimes_R B'$ respectively, then $(\operatorname{coker} l', g'')$ is the tensor product $A \otimes_R \operatorname{coker} l$.



Proof. Let C be an abelian group, and let $f : A \times \operatorname{coker} l \longrightarrow C$ be an R-bilinear map. We want to show that there exists a unique group homomorphism $\phi : \operatorname{coker} l' \longrightarrow C$ that makes the diagram above commute. The composed map $\tau = (\mathrm{id}_A, \mathrm{can}_B) \circ (\mathrm{id}_A, l)$ has $A \times 0$ as image. By R-bilinearity of f we conclude that $h = f \circ \tau$ is the zero map. We are also given the unique group homomorphisms ϕ_1 and ϕ_2 as seen in the diagram. Our map ϕ_1 is the zero map because h is the zero map. By the homomorphism theorems we conclude that ϕ_2 factors through the cokernel of l. This gives us a unique homomorphism $\phi : \operatorname{coker} l' \longrightarrow C$ with the property that $\phi \circ \mathrm{can}_D = \phi_2$. It now remains to show that $f = \phi \circ g''$. Since the mapping $(\mathrm{id}_A, \mathrm{can}_B)$ is surjective it is sufficient to show that $f \circ (\mathrm{id}_A, \mathrm{can}_B) = \phi_2 \circ g'$. But this is true by definition of ϕ_2.

For uniqueness, let ϕ' be another mapping such that $f = \phi' g''$. The composition of ϕ' and

the canonical map onto the cokernel of l' is ϕ_2 by uniqueness of ϕ_2. By the uniqueness of the factorisation of ϕ_2 we have proved that $\phi' = \phi$.

□

We can formulate this as $A \otimes_R (\text{coker} l) = \text{coker}(\text{id}_A \otimes_R l)$. We haven't talked yet about tensoring maps. We write l' as the tensor product of the maps id_A and l over R. Hence we see that taking the tensor product commutes with taking cokernels.

Thus we have seen that from fact 1 and fact 2 we can take tensor products of free modules. If we want to do general tensor products it suffices to prove that every module is isomorphic to the cokernel of a map between free modules. We can show this by construcing an exact sequence of R-modules

$$F' \xrightarrow{l} F \longrightarrow B \longrightarrow 0,$$

where F and F' are free R-modules. Because of fact 1 and fact 2 we derive that $A \otimes_R F$ and $A \otimes_R F'$ exist. The exact sequence gives us that B is isomorphic with the cokernel of l and hence due to fact 3, that the tensor product $A \otimes B$ exists.

4.23. Example. The group $\mathbb{Z}/2\mathbb{Z}$ is certainly the cokernel of a map between free modules. Namely take $l : \mathbb{Z} \longrightarrow \mathbb{Z}$ with $z \mapsto 2z$. So if $B = \mathbb{Z}/2Z$ and $R = \mathbb{Z}$ we find that $A \otimes_R B = A/2A$.

To construct the exact sequence we take $S \subset B$ to be a set of generators (this exists because we can take $S = B$). We can now define a mapping

$$\begin{array}{ll} \phi : R^{(S)} & \longrightarrow B \\ (r_s)_{s\in S} & \longmapsto \sum_{s\in S} r_s s \end{array}$$

which is clearly surjective, giving us the following exact sequence:

$$R^{(S)} \xrightarrow{\phi} B \longrightarrow 0.$$

It remains to show that we can find a free module that maps onto the kernel of ϕ. To accomplish this we take $I \subset R^{(S)}$ a set of generators for the kernel of ϕ and define a mapping similar to ϕ:

$$\begin{array}{ll} \psi : R^{(I)} & \longrightarrow R^{(S)} \\ (r_i)_{i\in S} & \longmapsto \sum_{i\in I} r_i i. \end{array}$$

From these two maps we get the exact sequence:

$$R^{(I)} \xrightarrow{\psi} R^{(S)} \xrightarrow{\phi} B \longrightarrow 0.$$

This construction of the tensor product gives a lot of freedom since you are free to pick the generators that you want. The uniqueness statement at the beginning of this section (theorem 4.17) tells us that we will always end up with the same tensor product.

Chapter 5

Lecture 5

5.1 Properties of the tensor product

In this section, we will state some important properties of the tensor product. In most cases, we will leave (detailed) proofs to the reader.

5.1. Property. For every ring R, right modules A, A' and left modules B, B' and R-bilinear maps $f : A \to A'$, there is a unique group homomorphism $A \otimes B \xrightarrow{f \otimes g} A' \otimes B'$ sendig each $a \otimes b$ to $f(a) \otimes g(b)$.

5.2. Property. If $(e_i)_{i \in I}$ is a basis of B over R, then $A \otimes_R B = \bigoplus_{i \in I} (A \otimes e_i)$.

This is in fact a special case of the 'distributive law', see 4.21.

5.3. Property. $A \otimes \lim_{\to} B_i = \lim_{\to}(A \otimes B_i)$

This is exercise 68b.

5.4. Property.

$$B \xrightarrow{f} C \xrightarrow{g} D \longrightarrow 0.$$

is an exact sequence, then

$$A \otimes_R B \xrightarrow{\mathrm{id}_A \otimes f} A \otimes_R C \xrightarrow{\mathrm{id}_A \otimes g} A \otimes_R D \longrightarrow 0.$$

is also exact.

The proof of this statement follows immediately from the construction of the tensor product we gave in the previous chapter. We say 'tensoring is right-exact'. Remark that generally tensoring won't be left exact (this is exercise 69).

5.5. Property. If B is a submodule of C, then it's not generally true that $A \otimes_R B$ is the subgroup of $A \otimes_R C$ generated by $\{a \otimes b : a \in A, b \in B\}$.

To give an example: remark that $(\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$, the only non-trivial element being $1 \otimes 1$. So, naturally $(\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} (2\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$, the only non-trivial element being $1 \otimes 2$. But in $(\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/4\mathbb{Z})$, the element $1 \otimes 2$ is equal to zero.

5.6. Property. If $I \subset R$ is a right ideal, then $(R/I) \otimes_R B \cong B/(I \cdot B)$, where $I \cdot B$ is the subgroup of B generated by $\{ib : i \in I, b \in B\}$.

This follows from property 5.4. We have the exact sequence

$$I \longrightarrow R \longrightarrow R/I \longrightarrow 0.$$

which gives us the exact sequence

$$I \otimes_R B \xrightarrow{j \otimes b \mapsto i \otimes b} R \otimes_R B \longrightarrow (R/I) \otimes_R B \longrightarrow 0.$$

We know that $R \otimes_R B \cong B$, so we see by the exactness of the sequence that the kernel of the second map will be generated by the elements $i \otimes b : i \in I, b \in B$. In this case this kernel will be isomorphic to $I \cdot B$, this follows immediately from the definition of the map g in Fact 1 of the previous chapter.

5.7. Property. The map $f \otimes g$ from property 5.1 is $\mathbb{Z}$-bilinear in f and g, so $f \otimes (g_1 + g_2) = f \otimes g_1 + f \otimes g_2$ and $f \otimes (g \circ h) = f \otimes g \circ f \otimes h$.

5.8. Property. $A \otimes_R B \cong B \otimes_{R^{\mathrm{opp}}} A$, $a \otimes b \leftrightarrow b \otimes a$

The bilinear map $(x, y) \mapsto (y \otimes x)$ will do the job immediately.

5.9. Property. If A is an S-R-bimodule, and likewise B is an R-T-bimodule, then $A \otimes_R B$ has an S-T-bimodule structure through $s \cdot (a \otimes b) \cdot t = (sa) \otimes (bt)$ for all $s \in S$ and $t \in T$.

To prove this property, apply property 5.1 to the R-linear maps $f_s : A \to A$, $a \mapsto sa$ and $g_t : B \to B$, $b \mapsto bt$: then $f_s \otimes g_t : A \otimes_R B \to A \otimes_R B$, $(a \otimes b) \mapsto (sa) \otimes (bt)$ gives the desired structure.

5.10. Property. If A, B are like in the previous property, and C is a T-U-bimodule, then $(A \otimes_R B) \otimes_T C \cong A \otimes_R (B \otimes_T C)$, $(a \otimes b) \otimes c \leftrightarrow a \otimes (b \otimes c)$.

5.11. Property. If $R \to R'$ is a ring homomorphism, and B is an R-module, then $R' \otimes_R B$ is an R-module.

We know R' is an R'-R-bimodule, and B is a R-$\mathbb{Z}$-bimodule, so property 5.10 tells us that $R' \otimes_R B$ is an R'-$\mathbb{Z}$-bimodule, so an R'-module.
In this case, $R' \otimes_R B$ is said to be obtained from R by 'extension of scalars'.

5.12. Property. If $R \to R_1$, $R \to R_2$ are ring homomorphisms with $\mathrm{im}(R) \subset Z(R_i)$ for $i \in \{1, 2\}$, then $R_1 \otimes_R R_2$ has a unique ring structure satisfying $(a \otimes b) \cdot (a' \otimes b') = (aa') \otimes (bb')$. If we take groups G_1 and G_2, and let $R_1 = \mathbb{Z}[G_1]$ and $R_2 = \mathbb{Z}[G_2]$, we have a ring isomorphism

$$\mathbb{Z}[G_1] \otimes_{\mathbb{Z}} \mathbb{Z}[G_2] \cong \mathbb{Z}[G_1 \times G_2]$$

Apply property 5.10 and property 5.11 to prove this.

5.2 Induced modules

5.13. Definition. Let G be a group, $H \subset G$ a subgroup and L a G-module. Then L is said to be induced from H if there exists an H-module M and a G-module isomorphism

$$L \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M$$

Note that $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M$ is a $\mathbb{Z}[G]$-module by property 5.10, so in particular a G-module. Pick a set $P \subset G$ of left coset representatives for a subgroup $H \subset G$. This gives rise to a bijection $P \times H \to G$. We see that

$$\mathbb{Z}[G] \cong \bigoplus_{\sigma \in G} \mathbb{Z}\sigma \cong \bigoplus_{\rho \in P, \tau \in H} \mathbb{Z}\rho\tau \cong \bigoplus_{\rho \in P} \rho\mathbb{Z}[H]$$

So $\mathbb{Z}[G]$ is free as a right $\mathbb{Z}[H]$-module, with basis P. This means

$$\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M \cong \bigoplus_{\rho \in P} (\rho \otimes M)$$

For each element $x \in \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M$ there is a unique system $(x_\rho)_{\rho \in P}$ (with almost all components equal to zero) such that $x = \sum_{\rho \in P} \rho \otimes x_\rho$, by distributivity and the freeness of $\mathbb{Z}[G]$ as a $\mathbb{Z}[H]$-module.

This construction gives rise to a question: given a $\sigma \in G$, how to compute σx, i.e., how to compute $\sigma(\rho \otimes x_\rho)$? By property 5.11, we have $\sigma(\rho \otimes x_\rho) = (\sigma\rho) \otimes x_\rho$. We know that $\sigma\rho = \rho'\tau$ for some $\rho' \in P, \tau \in H$, so we have $(\sigma\rho) \otimes x_\rho = (\rho'\tau) \otimes x_\rho = \rho' \otimes \tau x_\rho$ because the tensor product was taken over $\mathbb{Z}[H]$. Hence we have made $\sigma(\rho \otimes x_\rho)$ into an element we can compute.

5.14. Theorem. Let G be a group, $H \subset G$ a subgroup, P a system of left coset representatives, L a G-module. Then L is induced from H if and only if L has an H-submodule M such that the map

$$\bigoplus_{\rho \in P} \rho M \xrightarrow{\Sigma} L$$

given by summation is a bijection.

Proof

'$\Longrightarrow$': If L is induced, we know that $L \cong \bigoplus_{\rho\in P}(\rho \otimes J)$ with J some H-module. Note that J is a submodule of L, by the map $J \leftarrow 1 \otimes J$ (check that this subgroup of $\bigoplus_{\rho\in P}(\rho \otimes J)$ is indeed an H-module). Also note that $\bigoplus_{\rho\in P}(\rho\otimes J) \to \bigoplus_{\rho\in P} \rho J$ given by the natural map is an isomorphism of G-modules. We also know that for each element $x \in \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M$ there is a unique system $(x_\rho)_{\rho\in P}$ with almost all components to zero such that $x = \sum_{\rho\in P}(\rho\otimes x_\rho)$. Now we just take $M = J$, and we see that Σ is a bijection.

'$\Longleftarrow$': We now there exists a map $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M \to L$ given by $r \otimes x \mapsto rx$, and this map is $\mathbb{Z}[G]$-linear, so a G-map in particular. We also know that

$$\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M \cong \bigoplus_{\rho\in P}(\rho \otimes M) \cong \bigoplus_{\rho\in P} \rho M$$

and we are given that the map $\bigoplus_{\rho\in P} \rho M \xrightarrow{\Sigma} L$ is a bijection. Combining these notions, we see that the map $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M \to L$ given by $r \otimes x \mapsto rx$ must be a bijection, so L is induced. □

Chapter 6

Lecture 6

6.1 The wreath product

To prove the main theorem 1.19 we will also be needing the concept of a wreath product. Let us start with a definition.

6.1. Definition. Let H and G be groups and let G act on a set X. Define the action of G on the direct product H^X by

$$^{\sigma}f(x) = f(\sigma^{-1}x),$$

for all $f \in H^X$, $x \in X$, and $\sigma \in G$. We then define the wreath product of H and G, relative to the action of G on X, as the semidirect product of H^X and G, which we write as $H \wr_X G$ or $H \wr G$ if the set on which G acts is understood.

So the wreath product of the groups H and G is again a group. An element of a wreath product $H \wr_X G$, looks like a 2-tuple (f, σ) with f a function from X to H and $\sigma \in G$. We can derive the group operation from the definition above and find that $(f, \sigma) \cdot (g, \tau) = (f^{\sigma} g, \sigma\tau)$ where $(f^{\sigma} g)(x) = f(x)g(\sigma^{-1}x)$. From this perspective we can see that

$$\#H \wr_X G = \#H^{\#X} \cdot \#G$$

(which also makes sense if either of the groups, or the set, has infinite cardinality).

6.2. Remark. Suppose that Y is an H-set. Then $H \wr_X G$ acts on $Y \times X$ by

$$(f, \sigma) \cdot (y, x) = (f(\sigma x) \cdot y, \sigma x)$$

If G acts on X, we will frequently use the following notation:

$$G|_X = \{ \text{ image of } G \text{ in } \mathrm{Sym}(X) \ \}.$$

Also recall that by G_x we mean the stabilisor of x in G.

6.2 Finding a bound

We now give a theorem whose relevance will become clear soon.

6.3. Theorem. Let Γ be a group, let Z and X be Γ-sets with $Z \neq \emptyset$ and X transitive, and let $p : Z \to X$ be a Γ-map and $x_0 \in X$. Put $Y = p^{-1}(x_0)$, $G = \Gamma|_X \subset \mathrm{Sym}(X)$, $H = \Gamma_{x_0}|_Y \subset \mathrm{Sym}(Y)$. Then the set

$$\Delta = \{\tau \in \mathrm{Sym}(Z) : \exists \tau' \in G : \tau' p = p\tau, \text{ and } \forall x \in X : \exists \tau_x \in \Gamma : \forall z \in p^{-1}(x) : \tau z = \tau_x z\}$$

is a subgroup of $\mathrm{Sym}(Z)$ with $\Gamma|_Z \subset \Delta$ and there exists a group isomorphism $\Delta \xrightarrow{\sim} H \wr_X G$ plus a bijection $Z \xrightarrow{\sim} Y \times X$ that are compatible, i.e., making the following diagram commutative.

$$\begin{array}{ccc} \Delta \times Z & \xrightarrow{\text{obvious action of } \Delta \text{ on } Z} & Z \\ \downarrow \wr & & \downarrow \wr \\ (H \wr_X G) \times (Y \times X) & \xrightarrow{\text{as in remark 6.2}} & Y \times X. \end{array}$$

Proof. We will not give a rigorous proof but outline the general idea. To show that Δ is a subgroup one only has to follow his nose. For example, for closedness under the group operation, take $a, b \in \Delta$. It is given that a' and b' exist such that $a'p = pa$ and $b'p = pb$. One easily checks that $a'b'$ is the element in G such that $a'b'p = pab$. The other property goes analogously. The existence of inverses follows directly from the existence of inverses in G and Γ.

The second statement that $\Gamma|_Z$ is a subset of Δ is also trivial since for any element $\tau \in \Gamma|_Z$ we can just take $\tau' = \tau$ and $\tau_x = \tau$ for all x to conclude that $\tau \in \Delta$.

To show there is a group isomorphism it is best to first write down the bijection $Z \xrightarrow{\sim} Y \times X$. We choose, for each $x \in X$, a $\sigma_x \in \Gamma$ such that $\sigma_x x_0 = x$ (this might require the axiom of choice). Such a choice gives us a map

$$\begin{array}{rccc} \phi : & Y \times X & \longrightarrow & Z \\ & (y, x) & \longmapsto & \sigma_x y. \end{array}$$

This is easily verified to be a bijection by checking it for each of the fibers of the elements of X (hence ϕ^{-1} is the claimed bijection in the theorem). Now look at the following diagram.

$$\begin{array}{ccccc}
\Delta & \subset & \mathrm{Sym}(Z) & & \tau \\
\big| \wr & & \big| \wr & & \big| \\
(\text{image of } \Delta) & \subset & \mathrm{Sym}(Y \times X) & & \phi^{-1}\tau\phi \\
\| & & & & \\
H \wr_X G & \ni & ((\rho_x)_{x\in X}, \rho'). & &
\end{array}$$

We can identify the symmetries of Z with those of $Y \times X$ by renumbering through ϕ. Also we see that Δ acts on $\mathrm{Sym}(Z)$, and by transport of structure, it also acts on $\mathrm{Sym}(Y \times X)$. It remains to show that the image of Δ, or $\Delta|_{Y\times X}$ as we have written, is exactly the wreath product $H \wr_X G$ that in this particular case is acting faithfully on $Y \times X$. One can now verify, that picking an element in the image of Δ exactly determines an element in the wreath product. So we have ρ_x for each x corresponding to the τ_x in the definition of Δ, and ρ' corresponding to τ' in the definition of Δ. We leave these verifications to the reader. □

Let's look at some consequences of the theorem.

6.4. Corollary. Under the same hypotheses as the previous theorem, with Z and X finite, one has

$$(\#\Gamma|_Z) \mid (\#H^{\#X} \cdot \#G).$$

The following corollary will give us a bound for the size of transitive permutation groups in terms of the primitive case. It will be a much weaker statement than the main theorem 1.19 since we only require transitivity of G and not primitivity. In some sense, we can view it as factoring G and X into more managable pieces (for determining an upper bound).

6.5. Corollary. Let G be a finite solvable group acting faithfully and transitively on a set X. Then, for some $t \in \mathbb{Z}_{\geq 0}$, there are finite solvable groups $G_1, \ldots, G_t$ and these groups are acting faithfully and <u>primitively</u> on the sets $X_1, \ldots, X_t$ (G_i acts on X_i) such that $\#X = \prod_i \#X_i$ then

$$\#G \mid \prod_{i=1}^{t} \#G_i^{\prod_{j=i+1}^{t} \#X_j}, \tag{6.6}$$

where by convention the empty product equals 1.

Proof. We proceed by induction on the cardinality of X.

If $\#X = 1$ (this is the minimal cardinality of X since G acts transitively) then $\#G = 1$ since G acts faithfully on one element. We then take $t = 0$ and there is not much left to verify.

If X is primitive, then we can take $t = 1$ and $G_1 = G$ and $X_1 = X$ and one again easily verifies the claims in the corollary.

We now consider the case that X is non-primitive and split X up into smaller parts to which we can apply the induction hypothesis. First, pick a G-invariant equivalence relation $\sim$ on X with the smallest number (> 1) of equivalence classes. Now we will try to apply theorem 6.3. Let us first check some conditions. The set $X/\sim$ is a transitive set because X is transitive. Our group G acts on $X/\sim$ precisely because the equivalence relation was chosen to be G-invariant. Also, we have a map $p : X \to X/\sim$ that sends an element x to its equivalence class $[x]$, which is certainly a G-map. Now pick an equivalence class $[x_0]$. This gives us a fiber, say $Y = p^{-1}([x_0])$, and a group H that acts on Y in a faithful way. From the theorem, and more particularly, from corollary 6.4, we have that

$$\#G \mid (\#H)^{\#X} \cdot \#(G|_{X/\sim}). \tag{6.7}$$

The action of G on $X/\sim$ is primitive. Otherwise, we could lift the non-trivial equivalence relation begotten from non-primitivity of $X/\sim$ and lift it to X giving us another G-invariant equivalence relation on X with a smaller number of classes, contradicting what we have demanded of $\sim$.

Because H is G modulo some normal subgroup of G we see that H is solvable. Also, H acts faithfully on the fiber Y. Because the action of G on X is transitive, it follows easily that the action of H on Y is also transitive. Hence, we can invoke the induction hypothesis since $\#Y < \#X$ since the number of equivalence classes in $X/\sim$ is greater than one, and get $X_1, X_2, \ldots, X_{t-1}$, and $G_1, G_2, \ldots, G_{t-1}$ that satisfy the formula in 6.6 for $t-1$ and H.

We can then take $X_t = X/\sim$ and $G_t = G|_{X/\sim}$. By using formula 6.7 we see that equation 6.6 indeed holds for all the X_i and G_i. □

6.8. Remark. This is a result that in this generality cannot be improved. If one starts with t groups, all being finite and solvable, acting respectively on t sets, faithfully and primitively, then by applying the wreath product construction inductively, one can produce a group that is finite solvable, acting on the product of the sets for which the order takes exactly the upper-bound as given in formula 6.6.

6.3 Wreath products and modules

As we have seen in the previous section, we looked at a set Z that was broken up into a disjoint union of fibers: $\coprod_{x\in X} p^{-1}(x)$. Now we are going to do this in terms of modules. However, we will not be building a big set out of small sets by taking the disjoint union, we will build a big module M out of small modules. But the disjoint union of modules is not a module, so we will take the direct sum $M = \bigoplus_{x\in X} N_x$. This is just a brief motivation. Let us work out the details.

Let G and H be groups and X a G-set. Let N be an H-module. We then have that $N^{(X)} = M$ becomes a module over the wreath product by

$$(f, \sigma) \cdot y : x \mapsto f(x) \cdot y(\sigma^{-1}x)$$

with $y \in N^{(X)}$, $f \in H^X$, and $\sigma \in G$. So how do we understand this action of the wreath product? We can get an idea by fixing the first component, and taking f to be the trivial map, mapping everything to the unit element. The action then comes down to sending an element x to $y(\sigma^{-1}x)$. This basically means that it permutes the summands of an element $y \in M = \sum_{x\in X} N_x$. The other way around, fixing $\sigma = 1$, we see that x is sent to $f(x) \cdot y(x)$. This just says that H^X acts on $N^{(X)}$ since H acts on N on each coordinate (the x-th coordinate of H acts on the x-th coordinate of N).
Now let us look at another theorem and note the similarities with theorem 6.3.

6.9. Theorem. Let Γ be a group, X a transitive Γ-set, and M a Γ-module with non-zero subgroups $N_x \subset M$, one for each $x \in X$, such that $\bigoplus_{x\in X} N_x \xrightarrow{\sim} M$ is an isomorphism given by $(n_x)_{x\in X} \mapsto \sum_{x\in X} n_x$, and such that

$$\forall x \in X, \sigma \in \Gamma : \sigma N_x = N_{\sigma x}.$$

Let $x_0 \in X$, and put $N = N_{x_0}$, $G = \Gamma|_X \subset \mathrm{Sym}(X)$, $H = \Gamma_{x_0}|_N \subset \mathrm{Aut}(N)$ and

$$\Delta = \{\tau \in \mathrm{Aut}\ M : \exists \tau' \in G\ \forall x \in X : \tau N_x = N_{\tau' x}, \forall x \in X : \exists \tau_x \in \Gamma : \forall z \in N_x : \tau z = \tau_x z\}$$

(considering $\mathrm{Aut}(M)$ as an abelian group). Then $\Delta \subset \mathrm{Aut}(M)$ is a subgroup. Also, $\Gamma_M \subset \Delta$ is a subgroup (this will give us an upper bound for Γ) and there are compatible group isomorphisms $\Delta \xrightarrow{\sim} H \wr_X G$, $M \xrightarrow{\sim} N^{(X)}$, i.e., making the following diagram commutative.

$$\begin{array}{ccc} \Delta \times M & \longrightarrow & M \\ \downarrow\wr & & \downarrow\wr \\ (H \wr_X G) \times N^{(X)} & \longrightarrow & N^{(X)}. \end{array}$$

Proof. We leave the proof of the theorem to the reader and note that it goes completely analogously to theorem 6.3. Here, M plays the role of Z, the N_x's play the role of the fibers $p^{-1}(x)$, and $N = N_{x_0}$ takes the role of Y. □

This gives rise to a corollary which enables us to say something about simple modules in terms of primitive modules which is defined as follows.

6.10. Definition. Let G be a group and N a G-module, then N is called primitive if

- N is simple as a G-module;
- N is not induced from any subgroup $H \subsetneq G$.

It is analogous to concept of primitive G-sets where the first condition corresponds to the transitivity. Remember that N is induced if we can write it as

$$\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} P = \bigoplus_{\sigma H \in G/H} \sigma P$$

with P an H-module. So if N is simple but not induced, it cannot be of this form except if X has just one element. Hence, if N is simple but not primitive, we can split into a direct sum and otherwise the theorem applies. If it is simple and primitive, then there are other ways of controlling the cardinality. We will now give a theorem that will allows us to control the size of simple modules through primitive modules.

What we did in corollary 6.5 was break a group and a set X up into groups acting on smaller sets. In the following corollary we have H and G instead of a whole sequence of groups, and we have an H-module N and a faithful G-set X instead of a whole sequence of sets. Note that, unlike before, our set X is only transitive and not primitive. If you want to make the G-set X also primitive then you have to apply corollary 6.5.

6.11. Corollary. Let Γ be a finite solvable group and M a faithful simple Γ-module. Then there exist finite solvable groups H and G, a faithful primitive H-module N, and a transitive faithful G-set X such that $\#M = (\#N)^{\#X}$, $\#\Gamma \mid (\#H)^{\#X} \cdot \#G$.

Proof. The proof is similar to the proof of 6.5. However, it is much simpler since there is no induction step required. Pick $B \subset \Gamma$ a minimal subgroup such that M is induced from B and put $X = \Gamma/B$. The reason this minimal subgroup exist is because there is at least one such subgroup, namely Γ itself, and because Γ is finite, so that there will indeed by a minimal one. In the case that B is indeed equal to Γ, this says that M is primitive. In that case we are done since we can take $G = 1$, $H = \Gamma$, and X will only have one element. One easily verifies the claim in the theorem.

So then assume that $B \neq \Gamma$. We then have that M is induced from B meaning that it can be written as

$$M = \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[B]} N = \bigoplus_{\sigma B \in X} \sigma N$$

with N a $\mathbb{Z}[B]$-module. One easily checks that the conditions for theorem 6.9 are satisfied (with σN as the N_x's and $H = B|_N$). So the order of Γ, which is acting on M, and which in this case is all of Γ since M is faithful, divides the order of Δ, which is the order of the wreath product: $\#H^{\#X}$. The only left to verify is that N is primitive as a $\mathbb{Z}[B]$-module.

Suppose that N has a non-trivial submodule N'. Then $M' = \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[B]} N'$ is a non-trivial submodule of M: contradiction with the simpleness of M. Also, if N induced from $A \subset B$, then $N \cong \mathbb{Z}[B] \otimes_{\mathbb{Z}[A]} P$ with P some $\mathbb{Z}[A]$-module. But then we can write $M = \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[B]} \mathbb{Z}[B] \otimes_{\mathbb{Z}[A]} P$ (parentheses omitted due to associativity of the tensor product) or $M = \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[A]} P$ and hence M is induced from A giving us $A = B$ since B was the smallest subgroup from which M was induced. So we see that N is not induced from a proper subgroup. This proves that N is a primitive $\mathbb{Z}[B]$-module and at the same time proves that N is a primitive $\mathbb{Z}[H]$-module because B is just the way H is acting upon N. □

6.4 A little road map

We will briefly discuss what we have done so far in order to prove our maine theorem 1.19 and what still remains to be done. First let us look at what remains to be done:

- for a finite solvable group G and a faithful primitive G-module M, estimate $\#G$ as a function of $\#M$;
- put everything together

So in theorem 1.19 we are starting with a primitive G-set X (with G solvable and G acting faithfully, this will be the case from now on so we will not mention it again). We have then reduced this with theorem 2.18 to a simple H-module (with H a subgroup of our original G). If we can solve it for this simple module, then we can solve it for the original case. So the next step is getting the bound for the simple module. This is done by using the corollary above. For this we have to do two things. Firstly, we have to control primitive G-modules (not for our original G, but we will just call it G for simplicity). Secondly, to control the case of a transitive G-set because we want to estimate the size of this G in terms of the transitive set that it is acting upon. The G is controlled by X and H by N and together this gives us our bound.

This means that we have replaced our original problem by a harder one since every primitive set is also transitive but not the other way around. So what do we do in this case? We replace our transitive G-set, say X, by a whole sequence of groups, and a whole sequence of primitive sets begotten from corollary 6.5. So in order to solve our problem, we have to solve our problem! The big gain however, is that the G-sets we end up with through corollary 6.5 are tiny (with respect to cardinality) in comparison to our original G-set X.

Chapter 7

Lecture 7

7.1 The last pieces of the puzzle

We will begin with a theorem.

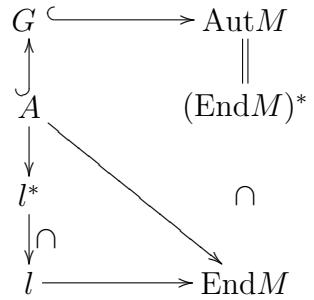
7.1. Theorem. Let G be a finite solvable group, M a faithful primitive G-module and A an abelian normal subgroup of G. Then

(a) A is cyclic;

(b) the subring l of $\mathrm{End}(M)$ that is generated by the image of A is a field;

(c) if $\#l = p^n$ (p prime, $n \in \mathbb{Z}_{>0}$) then $(G : C_G(A))|n$ with $C_G(A) = \{g \in G : \forall a \in A : ga = ag\}$ the centralizer of A in G, and $\#A|p^n - 1$.

Proof. We will first draw a little diagram showing some of the relations between the objects. Since G is acting on M, we can consider the map from G to Aut M. Note that this is an injection as M is a faithful G-module. We will therefore identify elements of G with automorphisms of M.



We will first view M as a module over A instead of over G. This is easier to work with since A is abelian and we know more about modules over commutative rings. Since M

is primitive as a G-module, we have $M \neq 0$. Choose a minimal non-zero sub-l-module M' of M. Then M' is simple as an l-module, so $M' \cong l/\underline{\mathfrak{m}}$ with $\underline{\mathfrak{m}} \subset l$ a maximal ideal (we should say left-ideal, but l is commutative so this makes no difference). Now $M[\underline{\mathfrak{m}}] = \{x \in M : \forall r \in \underline{\mathfrak{m}} : rx = 0\}$ is a sub-l-module of M containing M' so $M[\underline{\mathfrak{m}}] \neq 0$.

For $\sigma \in G$, $r \in$End M we write ${}^{\sigma}r = \sigma r \sigma^{-1}$ (multiplication is done within End M). So if $x \in M$, then ${}^{\sigma}r(\sigma x) = \sigma r x$. Then ${}^{\sigma}\underline{\mathfrak{m}}$ is a maximal ideal of ${}^{\sigma}l = l$ (this equality holds because A is normal in G), and $M[{}^{\sigma}\underline{\mathfrak{m}}] = \sigma M[\underline{\mathfrak{m}}] \neq 0$.

Now put $H = \{\sigma \in G : {}^{\sigma}\underline{\mathfrak{m}} = \underline{\mathfrak{m}}\}$, the stabilizer of $\underline{\mathfrak{m}}$. The number of different ${}^{\sigma}\underline{\mathfrak{m}}$'s equals $(G : H)$. The claim is that the following map

$$\begin{array}{rll} f: & \bigoplus_{\sigma H \in G/H} M[{}^{\sigma}\underline{\mathfrak{m}}] & \longrightarrow M \\ & (a_1, \ldots, a_k) & \longmapsto \sum_k a_k. \end{array}$$

is a group isomorphism. It is clear that this is a group homomorphism. The image is non-zero ($M[\underline{\mathfrak{m}}] \neq 0$) and $\sum_{\sigma} \sigma M[\underline{\mathfrak{m}}]$ is a sub-G-module generated by $M[\underline{\mathfrak{m}}]$. Since M is simple, we conclude that the image must be all of M because otherwise the image would be a non-trivial sub-G-module. Injectivity is proved in exercise 91b. This proves the claim.

This gives us as a result that M is the direct sum of all $\sigma M[\underline{\mathfrak{m}}]$ with $\sigma H \in G/H$. But this means that M is induced from H (see theorem 5.14). Since M is primitive, our group H cannot be a proper subgroup of G so that $H = G$. Having shown that f is a group isomorphism then shows that $M = M[\underline{\mathfrak{m}}]$ which means that $\underline{\mathfrak{m}}$ annihilates M which can only happen if $\underline{\mathfrak{m}} = \{0\}$. This tells us that $l = l/\underline{\mathfrak{m}}$ impying that l is a field proving (b). Now (c) is also easily proved. Since l is a finite field, we can choose p and n such that $\#l = p^n$. We have that A is a subgroup of l^* which is the multiplicative group of order $p^n - 1$ of the finite field l. This gives us the last part of (c). Part (a) is clear since finite subgroups of the multiplicative group of a field are cyclic and hence A is cyclic.

It remains to prove the last part of (c). Look at the map ϕ from G to the field automorphism of l:

$$\begin{array}{rll} \phi: & G & \longrightarrow \text{Aut } l \\ & \sigma & \longmapsto (r \mapsto {}^{\sigma}r) \end{array}$$

The kernel are precicely the elements of G that commute with all elements of l. But since l is generated by the image of A, it follows that the kernel is the set of elements of G that commute with each element of A, or $\ker \phi = C_G(A)$. Since we have $G/\ker \phi \cong \text{im } \phi$, and because im ϕ is a subgroup of the field automorphisms of l which is a group of order n generated by the Frobenius automorphism, we automatically get that $(G : C_G(A))|n$. This proves the last part of the theorem. □

7.2. Example. Take $G = \mathrm{GL}(2, \mathbb{F}_3)$, $M = (\mathbb{F}_3)^2$ a vector space of dimension 2. Let G act on M by just multiplying a vector with a matrix. To determine the order of G we note that the first row can be anything except for $(0, 0)$ giving us 8 choices. Having made the choice for the first row, the second row cannot be a multiple of the first row, giving us $9 - 3 = 6$ choices. This gives a total order of 48. Since the smallest non-solvable group has order 60, this proves in a somewhat crude way that G is solvable. Also, M is a faithful G-module: only the identity matrix acts as the identity. It is also primitive (see exercise 97). Now G only has two abelian normal subgroups. Namely, the trivial one, and $\{\pm I\}$. If we take the latter case, we see indeed that A is cyclic, that the subring that it generates is a field: $\mathbb{F}_3$. We take $p = 3$ and $n = 1$ and then the statement about the index is also trivial. Of course this a rather trivial example, but you cannot blame the theorem for this, since the theorem basically says that all such examples will be trivial.

The next theorem will be about solvable groups that have the property that we get out of the previous theorem. Namely, that we have a maximal normal subgroup that is cyclic. We are going to use this to, so to speak, rip the entire group apart. The precise statement will become clear soon.

7.3. Theorem. Let G be a finite solvable group, let A be a maximal abelian normal subgroup, let C be the centralizer of A, and let B be a subgroup that is maximal among the set S of all subgroups H of G satisfying 3 conditions:

(a) H is normal in G;

(b) $A \subset H \subset C$;

(c) H/A is abelian.

(note that S is not empty since A is an element of it). Assume A is cyclic. Then we have $1 \subset A \subset B \subset C \subset G$ with $A, B, C \lhd G$ and there are two injective group homomorphisms

$$\begin{array}{rccl} f: & G/C & \longrightarrow & \mathrm{Aut}\ A \\ & \sigma C & \longmapsto & (\alpha \mapsto \sigma\alpha\sigma^{-1}) \end{array}$$

and

$$\begin{array}{rccl} g: & C/B & \longrightarrow & \mathrm{Aut}\ B/A \\ & \gamma B & \longmapsto & (\beta A \mapsto \gamma\beta\gamma^{-1}A) \end{array}$$

and also a group isomorphism

$$\begin{array}{rccl} h: & B/A & \xrightarrow{\sim} & \mathrm{Hom}(B/A,\, A) \\ & \beta A & \longmapsto & (\delta A \mapsto \beta\delta\beta^{-1}\delta^{-1}) \end{array}$$

which we will refer to as the self-duality of B/A. Also, we have that the exponent of B/A divides the order of A.

Proof. First, we will show that f is an injective group homomorphism. We look at the group homomorphism $G \longrightarrow \text{Aut } A$ defined by $\sigma \mapsto (\alpha \mapsto \sigma\alpha\sigma^{-1})$ which has kernel C by definition (since C is the centralizer of A in G). This means that C is normal in G and therefore G/C goes injectively into Aut A:

$$\begin{array}{ccc} G & \longrightarrow & \text{Aut } A \\ & \searrow \quad \nearrow & \\ & G/C & \end{array}$$

Since S is a finite set, this guarantees us that B indeed exists. The inclusions $1 \subset A \subset B \subset C \subset G$ are clear. By hypothesis A and B are normal, and we just proved that C is normal so that proves those statements. Now we will prove that h is an isomorphism.

The group B/A is abelian giving us that $[B, B] \subset A \subset Z(B)$ (since $B \subset C$). Exercise 43 tells us that $B \times B \longrightarrow A$, given by $(\beta, \delta) \longrightarrow \beta\delta\beta^{-1}\delta^{-1}$, is bilinear. This already gives us the following homomorphism ψ

$$\begin{array}{ccc} B & \xrightarrow{\psi} & \text{Hom } (B, A) \\ \downarrow & \overset{\psi'}{\searrow} & \uparrow i \\ B/A & \xrightarrow{\phi} & \text{Hom } (B/A, A) \end{array}$$

with $\psi : \beta \mapsto (\delta \mapsto \beta\delta\beta^{-1}\delta^{-1})$. That this is a group homomorphism follows from the fact that we can fix the first component in the map $B \times B \longrightarrow A$ and then get a group homomorphism in the second component. Consider the diagram above with i just the inclusion. For any $\delta \in A$, we have $[\beta, \delta] = 1$ since $A \subset Z(B)$. This means that all the group homomorphisms in the image of ψ are trivial on A. And these group homomorphisms are clearly the same as the group homomorphisms between B/A and A which are both abelian groups. This already gives us a group homomorphism ψ'. But also, if $\beta \in A$, then we also get that $[\beta, \delta] = 1$ since $A \subset Z(B)$. So if we look at the homomorphism ψ', we see that A is in the kernel. We can then look at the group homomorphism ϕ. The claim is that this is in fact a group isomorphism.
The kernel of ϕ equals the set of cosets of B/A, consisting of all elements that commute with all $\delta \in B$, so this is $Z(B)/A$. Because $A \subset Z(B)$ and since $Z(B)$ is also an abelian normal subgroup of G (it is a characteristic subgroup of the normal subgroup B, see exercise 4d), we must have $A = Z(B)$ by maximality of A. This proves that ϕ is injective. This means that there are at least $\#(B/A)$ homomorphisms. By proving exercise 94 one gets the reverse inequality, proving surjectivity. The exercise also tells us, that in the case of equality (which we have here), our group A is abelian (which we already knew), but also that the exponent of B/A divides the order of A, which was to be proved.

It only remains to show that g is a well-defined injective homomorphism. We will adopt the following notation: $\overline{N} = N/A$, and $\overline{\sigma} = \sigma A$. Consider the group homomorphism $g' : \overline{C} \longrightarrow \text{Aut } \overline{B}$ given by $\overline{\gamma} \mapsto \overline{\gamma}\overline{\beta}\overline{\gamma^{-1}}$ with kernel $\overline{D} \supset \overline{B}$. This induces a group homo-

morphism $g : \overline{C}/\overline{B} \longrightarrow \text{Aut } \overline{B}$ where $\overline{C}/\overline{B} = C/B$. We want to show that $\overline{D} = \overline{B}$ or that $D = B$ with D the preimage of $\overline{D}$ in G. This will prove that our map g is injective. We will do this by using the maximality of B. We know that D contains B, but also that B was maximal with the 3 properties (a), (b), and (c) that were stated in the theorem. We would like to go on to show that D also satisfies those properties and hence conclude that $D = B$. Surely, D is normal since $\overline{D}$ is a kernel and hence normal. Also, we have $1 = \overline{A} \subset \overline{D} \subset \overline{C}$ so that also $A \subset D \subset C$. This means D satisfies properties (a) and (b). But there is no clear reason why $\overline{D}$ should be abelian (property (c)). This is where we will use the solvability of G.

Suppose for a contradiction that $D \supsetneq B$ (or $\overline{D} \supsetneq \overline{B}$). Then D/B is non-trivial and solvable. In the chain of subgroups begotten by succesively modding out a group by its commutator subgroup starting with D/B, the last step, before getting the trivial subgroup will be characterstic. So, we conclude that D/B, has a non-trivial abelian characteristic subgroup, say E/B. We are thus in the situation where we have the following inclusions: $1 \subset A \subset B \subsetneq E \subset D \subset C \subset G$. To get our required contradiction, it suffices to show that

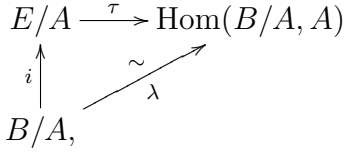
(1) E is normal;

(2) $A \subset E \subset C$;

(3) E/A is abelian.

Since if E satisfies these properties, then B was not maximal. Property (2) is obvious. To show that E is normal in G, we may as well divide out by the normal subgroup B and we look at $E/B \subset D/B \subset G/B$. Then, D/B is normal in G/B since D is normal in G and E/B is characteristic in D/B. Therefore, again by exercise 4d, we conclude that E/B is normal in G/B and hence that E is normal in G. This proves property (1). It now remains to show that property (3) holds. Look at the sequence $A \subset B \subset E$, we see that the first part B/A is abelian (we have shown this), and also we are given that E/B is abelian. Now we will show, using the self-duality of B/A that E/A is also abelian.

We have $E \subset D$ so that $\forall \epsilon \in E : g'(\overline{\epsilon}) = \text{id}_{\overline{B}}$ since $\overline{D}$ is the kernel of the map g'. This means that $\forall \epsilon \in E$ we have $\overline{\epsilon}\overline{\beta}\overline{\epsilon^{-1}} = \overline{\beta}$ or $[\overline{\epsilon}, \overline{\beta}] = \overline{\epsilon}\overline{\beta}\overline{\epsilon^{-1}}\overline{\beta^{-1}} = \overline{1}$. This means that $\forall \epsilon \in E, \forall \delta \in B : \epsilon\delta\epsilon^{-1}\delta^{-1} \in A$. This gives us that $[E, B] \subset Z(C)$. Since A is also contained in $Z(C)$ we can again invoke exercise 43. This tell us that the commutator map is bilinear. This gives us a homomorphism $E \longrightarrow \text{Hom}(B, A)$. Using similar arguments as in the beginning of the proof (with the map ψ), we see that we may as well regard this as a group homomorphism from E/A to $\text{Hom}(B/A, A)$. This gives us the diagram



with i the inclusion since B/A is sitting inside E/A. We can write the exact sequence

$$1 \longrightarrow B/A \longrightarrow E/A \longrightarrow E/B \longrightarrow 1$$

with $\lambda^{-1}\tau$ mapping $E/B \to E/A$.

that splits with the map $\lambda^{-1}\tau$. This gives us

$$E/A = B/A \oplus E/B,$$

which proves that E/A is abelian since B/A and E/B are both abelian. This contradicts the minimality of B and hence we conclude that $D = B$. This proves that the map g is injective, as was to be shown. □

7.2 The formulas

In this section we will take a bird's eye view and look at what we have done so far. We will also introduce some functions that will be used in the last lecture to give us the final bound for G in the main theorem 1.19 in terms of the size of X. The function that we are interested in is

$$P(n) = \max\{\#G : G \in S_1\}$$

with S_1 the class of all finite solvable groups for which there exists a faithful primitive G-set X with $\#X = n$. Theorem 1.19 claims that $P(n) \leq c_0 n^{c_1}$ for certain constants $c_0, c_1 \in \mathbb{R}_{\geq 1}$. Letting S_2 be the class of all finite solvable groups for which there exists a faithful simple module N with $\#N = q = p^k$, we define

$$S(q) = \max\{\#G : G \in S_2\}.$$

This function will be particularly useful because theorem 2.18 tells us that we can break up G into N, an elementary abelian group with the same cardinality as X, and a group H of order at most $S(\#N)$. So if $P(n)$ is defined, then n is a prime power and $P(n) = n \cdot S(n)$.

Now we define S_3 to be the class of finite solvable groups for which there exists a faithful primitive module N with $\#N = p^k = q$. We define

$$R(q) = \max\{\#G : G \in S_3\}.$$

Letting S_4 be the class of all finite solvable groups for which there exists a faithful transitive set X with $\#X = n$, we define

$$T(n) = \max\{\#G : G \in S_4\}.$$

Then corollary 6.11 shows that $S(q) = \max\{R(r)^k T(k) : r^k = q\}$. In the next lecture, we will see how to estimate $R(q)$ using the theorems from this lecture. Using corollary 6.5, we can bound $T(n)$ in terms of $P(q)$ by (empty product equals 1)

$$T(n) = \max\left\{ \prod_{i=1}^{k} P(q_i)^{\prod_{j=i+1}^{k} q_j} \;\middle|\; q_1, q_2, \ldots, q_k \text{ prime powers and } \prod_{i=1}^{k} q_i = n \right\}.$$

Note that the formulas for $S(q)$ and $T(n)$ are stated as an equality while the corollaries 6.11 and 6.5 give inequalities. This is because the groups in the corollaries (respectively Γ and G) can be seen as subgroups of some wreath product that is itself a group of the required type acting in the required way for which the upper-bound is assumed. See also remark 6.8.

Chapter 8

Lecture 8

8.1 Fitting the pieces together

8.1. Theorem. Let G be a finite solvable group and M a faithful primitive G-module. Then there are a prime number p and positive integers k and m, and normal subgroups $A \subset B \subset C$ of G such that:

1. $\#A | p^k - 1$
2. $\#B/A = m^2$
3. $\#C/B \leq m^{4 \log m / \log 2}$
4. $\#G/C | k$
5. $p^{km} | \#M$

We pick A, B, C as in 7.1: A is a maximal abelian normal subgroup of G, $C = C_G(A)$, B is maximal among $\{H \lhd G : A \subset H \subset C, H/A \text{ is abelian}\}$.
View G as a subgroup of $\operatorname{Aut} M = \operatorname{End}(M)^*$. In 7.1 we proved: the subring of $\operatorname{End}(M)$ generated by A is a finite field l, and $G/C \hookrightarrow \operatorname{Aut} L$. If we pick p and k such that $\#l = p^k$, we immediately see that 1 and 4 hold.

Now we are going to show that $\#B/A$ is a square. From 7.3 we know that $B/A \to \operatorname{Hom}(B/A, A), \beta A \mapsto (\delta A \mapsto \beta\delta\beta^{-1}\delta^{-1})$ is an isomorphism of abelian groups. Let D be a maximal abelian subgroup of B containing A. We have a map:

$$\begin{array}{ccc} B & \longrightarrow & \operatorname{Hom}(B, A) \\ & \overset{\varphi}{\searrow} & \downarrow \psi \\ & & \operatorname{Hom}(B/A, A) \end{array}$$

We know that ψ is surjective by exercise 95, and applying exercise 94 we see that $\#\mathrm{Hom}(D/A, A) = \#D/A$. Note: $D/A \subset \ker\varphi$ because D is abelian. Because D was chosen to be maximal, we have equality: if $\beta A \subset \ker\varphi$ then $\forall\delta \in D : \beta\delta\beta^{-1}\delta^{-1} = 1$ so $\beta\delta = \delta\beta$. This means that $D \cdot \langle\beta\rangle$ is also abelian, and D is contained in this group. By the maximality of D this group must be equal to D, so we have $\beta \in D$. This shows that $\ker\varphi = D/A$, and the isomorphism theorem gives us that

$$(B/A)/(D/A) \xrightarrow{\sim} B/D \xrightarrow{\sim} Hom(D/A, A)$$

We conclude that $\#(D/A) = (A : D) = \#(B/D)$, so this gives us that $(A : B) = (A : D)^2$, proving 2.

To prove 3, we recall that by 7.1: $C/B \hookrightarrow \mathrm{Aut}(B/A) = \mathrm{End}(B/A)^*$. If we say that $\langle x_1, \ldots, x_t\rangle$ is a minimal set of generators for B/A, this means:

$$\#(C/B) \leq \#\mathrm{Hom}(B/A, B/A) \leq m^{2t}$$

The second equality is justified by the fact that every group homomorphism is determined by the images of the generators, and for every element of this set we have at most m^2 choices by exercise 94. Because, if B/A can be generated by no less than t distinct elements, $\#B/A = m^2$ will be at least 2^t, we deduce that

$$t \leq \frac{\log(m^2)}{\log 2} = \frac{2\log m}{\log 2}$$

This tells us that $\#(C/B) \leq m^{2t} \leq m^{\frac{4\log m}{\log 2}}$, proving 3. It is possible to improve this bound, but this will require a lot of work, and this bound will be sufficient to prove our main theorem.

The last thing to do is proving the hardest part, 5. We know by 7.1 that $l \subset \mathrm{End}(M)$, so M is a vector space over l. This shows that 5 is equivalent to saying that $\dim_l M \geq m$, because $\#l = p^k$. The action of B on M is l-linear because $B \subset C = C_G(A)$. So M becomes an $l[B]$-module in which all elements of A act as scalars ($A \subset l^*$). Let $\bar{l}$ be an algebraic closure of l and $\overline{M} = \bar{l} \otimes_l M \cong \bar{l}^{(\dim_l M)}$ by Property 5.2 from chapter 5. This shows that $\dim_l M = \dim_{\bar{l}} \overline{M}$. Moreover, $\overline{M}$ is an $\bar{l}$-module by Property 5.11 from chapter 5, so automatically also an $\bar{l}[B]$-module (the action of B on $\overline{M}$ is defined naturally).

We are going to prove: $\dim_{\bar{l}} \overline{M} \geq m$. Let D such that $A \subset D \subset B$ be as before, so $B/D \xrightarrow{\sim} \mathrm{Hom}(D/A, A)$, $\beta D \mapsto \beta\delta\beta^{-1}\delta^{-1}$. Let $N \subset \overline{M}$ be a minimal non-zero $\bar{l}[D]$-module. Then N is a simple $\bar{l}[D]$-module, so $N \cong_{\bar{l}[D]} \bar{l}[D]/\mathfrak{m}$ with $\mathfrak{m} \subset \bar{l}[D]$ maximal. We know that D is abelian, so $\bar{l}[D]/\mathfrak{m}$ is a field, finite over $\bar{l}$. Hence we have $\bar{l}[D]/\mathfrak{m} \xrightarrow{\sim} \bar{l}$.

We have $D \lhd B$ (because $A \subset D \subset B$ and B/A is abelian), so $\bar{l}[D] \subset \bar{l}[B]$ and B acts on $\bar{l}[D]$ by ${}^\beta r = \beta r \beta^{-1}$. Note that $r \mapsto {}^\beta r$ is a ring automorphism of $\bar{l}[D]$. So ${}^\beta\mathfrak{m}$ is a maximal ideal of $\bar{l}[D]$ as well, it annihilates βN, i.e. $\beta N \subset \overline{M}[{}^\beta\mathfrak{m}]$.

8.2. Lemma. for $\beta \in B$, one has ${}^{\beta}\mathfrak{m} = \mathfrak{m}$ if and only if $\beta \in D$.

The 'if' implication is trivial since D is abelian.
To prove the other implication, note that for all $\delta \in D$ there exists a $\chi(\delta) \in \bar{l}^*$ such that $\delta - \chi(\delta) \in \mathfrak{m}$. Now we suppose that ${}^{\beta}\mathfrak{m} = \mathfrak{m}$. This means that $\forall \delta \in D : \beta(\delta - \chi(\delta))\beta^{-1} \in \mathfrak{m}$. Moreover:

$$\beta(\delta - \chi(\delta))\beta^{-1} = \beta\delta\beta^{-1} - \chi(\delta) = \beta\delta\beta^{-1}\delta^{-1}\delta - \chi(\delta)$$

We know that $\beta\delta\beta^{-1}\delta^{-1}$ is an element of A, so it is also an element of l^*. Now we see:

$$\beta\delta\beta^{-1}\delta^{-1}\delta - \chi(\delta) - (\delta - \chi(\delta)) = (\beta\delta\beta^{-1}\delta^{-1} - 1)\delta \in \mathfrak{m}$$

Because $\beta\delta\beta^{-1}\delta^{-1} - 1$ is a scalar, it is necessarily equal to zero, otherwise we find a unit element in a non-trivial ideal. So we conclude that $\beta\delta\beta^{-1}\delta^{-1} = 1$, so $\beta A \in \ker(B/A \to \mathrm{Hom}(D/A, A)) = D/A$. So $\beta \in D$. □

With this result we have found $\#B/D = m$ different maximal ideals ${}^{\beta}\mathfrak{m}$, each with the property that $\overline{M}[{}^{\beta}\mathfrak{m}] \neq 0$, because $\beta N \subset \overline{M}[{}^{\beta}\mathfrak{m}]$. Using exercise 91(b), we find the map $\bigoplus_{\beta} \overline{M}[{}^{\beta}\mathfrak{m}] \hookrightarrow \overline{M}$ So $\dim_{\bar{l}} \overline{M} \geq m$, so this concludes the last part of the theorem.

In the final part of the proof, P, R, S and T are as defined in the previous chapter.

8.3. Theorem. $R(p^d) \geq (p^d - 1) \cdot d$, with equality for all but finitely many pairs (p, d)

The '$\geq$' comes from $G = k^* \rtimes \mathrm{Aut}(k)$, with k a finite field with $\#k = p^d$.

If G, M, m, k are as in theorem 8.1, then we see

$$\#G = \#A \cdot \#B/A \cdot \#C/B \cdot \#G/C \leq (p^k - 1) \cdot m^2 \cdot m^{4 \log m / log 2} \cdot k$$

From 7.1(5) we know that $d \geq km$. If we can prove that

$$(p^k - 1) \cdot m^2 \cdot m^{4 \log m / \log 2} \cdot k \leq (p^{km-1}) \cdot km$$

holds for all but finitely many pairs (p, k) we are done, because $p^{km} - 1 \cdot km \leq (p^d - 1) \cdot d$. Clearly, there is some m_0 such that

$$m^{1+4 \log m / \log 2} \leq \frac{p^{km} - 1}{p^k - 1} = p^{(m-1)k} + \ldots + p^k + 1$$

is valid for all $m \geq m_0$. Moreover, it's clear that the inequality holds for $m = 1$. If $1 < m \leq m_0$, then $m^{1+4 \log m / \log 2} \leq p^{k(m+1)}$ for all but finitely many pairs (p, k). This proves the theorem.

Now it's clear there exists a constant c such that $R(p^d) \leq (p^d)^c$.

8.4. Theorem. There exists a constant c_1 such that $P(p^d) \leq (p^d)^{c_1}$ for all p, d. In fact, $c_1 = \frac{(c+1)\log 2 + \log 24}{\log 2 - \frac{2}{5}\log 5}$ will suffice.

We are going this theorem by induction on $q := p^d$. For $q = 2$ the statement clearly holds. Now suppose that $P(q') \leq q'^{c_1}$ for all $q' < q$, so $\log P(q') \leq c_1 \log q'$. We will first show that $T(n) \leq 2^{(c_1-c-1)\cdot n}$ for all $n < q$.
To do this, we are going to estimate

$$\frac{\log T(n)}{n} = \frac{\sum_{i=1}^{k} \log P(q_i)}{q_1 \dots q_i}$$

with $q_1 \dots q_k = n$. We are going to estimate every term of this sum. If $q_i \leq 4$ then

$$\frac{\log P(q_i)}{q_1 \dots q_i} \leq \frac{\log 4!}{2^i}$$

If $q_i \geq 5$, then by the induction hypothesis

$$\frac{\log P(q_i)}{q_1 \dots q_{i-1} q_i} \leq \frac{c_1}{2^{i-1}} \cdot \frac{\log q_i}{q_i} \leq \frac{c_1}{2^{i-1}} \cdot \frac{\log 5}{5}$$

because c_1 is positive. It turns out that

$$\frac{\log T(n)}{n} \leq \sum_{i \geq 1} \left(\frac{\log 4!}{2^i} + \frac{c_1}{2^{i-1}} \cdot \frac{\log 5}{5} \right) = \log 24 + \frac{2c_1}{5} \cdot \log 5 = (c_1 - c - 1) \cdot \log 2$$

Now we easily see that $T(n) \leq 2^{(c_1-c-1)\cdot n}$ for all $n < q$.

If we say that $q = p^k$, then

$$S(q) \geq R(p^d)^e \cdot T(e)$$

with for some pair $d, e \in \mathbb{Z}_{>0}$ such that $de = k$. Because $e \leq p^k$, we have

$$S(q) \geq (p^d)^e \cdot 2^{(c_1-c-1)\cdot e} \geq (p^d)^e \cdot (p^d)^{(c_1-c-1)\cdot e} = (p^{de})^{c_1-1} = q^{c_1-1}$$

Using the formula $P(q) = q \cdot S(q)$, we get that $P(q) = q^{c_1}$, so the induction is finished. This concludes the proof of our main theorem.

Chapter 9

Exercises

Solvable groups. Let G be a group. We define the sequence $G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \dots$ of subgroups of G inductively by $G^{(0)} = G$ and $G^{(i+1)} = [G^{(i)}, G^{(i)}]$. The group G is called *solvable* if $G^{(t)} = \{1\}$ for some $t \in \mathbf{Z}_{\geq 0}$.

Exercise 1. Let G be a group and let $H \subset G$ be a subgroup.
(a) Prove: if G is solvable, then H is solvable.
(b) Suppose H is normal in G. Prove: G is solvable if and only if H and G/H are both solvable.

Exercise 2. Let R be a ring, let n be a positive integer, and let G be the set of upper-triangular $n \times n$-matrices over R that have all diagonal entries equal to 1. Prove that G is a group under matrix multiplication, and that G is solvable.

Exercise 3. Let G be a group. Prove: G is solvable if and only if, for some non-negative integer k, there exists a sequence of subgroups $G = G_0 \supset G_1 \supset \dots \supset G_k = \{1\}$ of G such that for each $i = 0, \dots, k-1$ the group G_{i+1} is normal in G_i with G_i/G_{i+1} abelian, and if and only if, for some non-negative integer k, there exists a sequence of subgroups $G = G_0 \supset G_1 \supset \dots \supset G_k = \{1\}$ of G, all of which are normal in G, such that for each $i = 0, \dots, k-1$ the subgroup G_i/G_{i+1} of G/G_{i+1} is abelian.

Exercise 4. A subgroup H if a group G is called *characteristic* if for all $\phi \in \operatorname{Aut} G$ one has $\phi H = H$.
(a) Prove: each characteristic subgroup is normal.
(b) Prove that the commutator subgroup and the center of a group are characteristic subgroups.
(c) Give an example of a normal subgroup of a group that is not characteristic.
(d) Prove: a characteristic subgroup of a characteristic subgroup is characteristic, and a characteristic subgroup of a normal subgroup is normal.
(e) Give an example of a normal subgroup I of a normal subgroup H of a group G such that I is not normal in G.

Exercise 5. A group A is called *elementary abelian* if there is a prime number p such that A is isomorphic to the additive group of some vector space over $\mathbf{Z}/p\mathbf{Z}$.
Let G be a finite solvable group with $G \neq \{1\}$. Prove that G has a characteristic subgroup $A \neq \{1\}$ that is elementary abelian.

Exercise 6. A group G is called *characteristically simple* if G has exactly 2 characteristic subgroups (namely $\{1\}$ and G).
Let A be an abelian group. Prove: A is characteristically simple if and only if A is isomorphic to the additive group of some non-zero vector space over some field.

Group actions. Let G be a group and let X be a set. An *action* (or *left action*) of G on X is a map $G \times X \to X$, $(\sigma, x) \mapsto \sigma x$, such that for all σ, $\tau \in G$ and all $x \in X$ one has $(*)$ $\sigma(\tau x) = (\sigma\tau)x$ and $1x = x$; equivalently, it is a group homomorphism ϕ from G to the group $\operatorname{Sym} X$ of permutations of X, the connection between the two definitions being given by the formula $\sigma x = \phi(\sigma)(x)$ (for $\sigma \in G$, $x \in X$). If an action of G on X is given, we say that G *acts on* X. A *right action* of G on X is an action of the opposite group G^{opp} (see Exercise 7) on X. In the case of a right action, one usually writes $x\sigma$ instead of σx, so that the axiom $(*)$ for right actions reads $(x\sigma)\tau = x(\sigma\tau)$.

Exercise 7. Let G be a group. The *opposite* group G^{opp} has the same underlying set as G, the group multiplication $*$ on G^{opp} being defined by $\sigma * \tau = \tau\sigma$, for σ, $\tau \in G^{\mathrm{opp}}$. Prove that the groups G and G^{opp} are isomorphic.

Exercise 8. Let R be a ring. The *opposite* ring R^{opp} has the same underlying additive group as R, but with multiplication $*$ defined by $a * b = ba$, for a, $b \in R^{\mathrm{opp}}$.
(a) Prove that, for every positive integer n and every commutative ring A, the ring $M(n, A)$ of $n \times n$-matrices over A is isomorphic to its opposite.
(b) Is every ring isomorphic to its opposite? Give a proof or a counterexample.

Exercise 9. Let G be a group acting on two sets X and Y. Prove that G acts on the set Y^X of all maps $X \to Y$ by the formula $(\sigma f)(x) = \sigma f(\sigma^{-1}x)$ (for $\sigma \in G$, $f \in Y^X$, $x \in X$).

G-sets and G-maps. Let G be a group. A *G-set* is a set X together with an action of G on X. Let X and Y be G-sets. A *G-map* (or *G-equivariant map*) $X \to Y$ is a map $f\colon X \to Y$ with the property that for all $\sigma \in G$ and $x \in X$ one has $f(\sigma x) = \sigma f(x)$. Such a G-map is called a *G-isomorphism* if it has a two-sided inverse that is also a G-map or, equivalently, if it is bijective. If a G-isomorphism $X \to Y$ exists, we say that X and Y are *G-isomorphic*, notation: $X \cong_G Y$. A *G-automorphism* of X is a G-isomorphism from X to itself. The set of G-automorphisms of X is a group under composition, denoted by $\operatorname{Aut}_G X$.

Exercise 10. Let G be a group. If H is a subgroup of G, then we let G act on the set G/H of left cosets τH of H in G by the formula $\sigma(\tau H) = (\sigma\tau)H$.
Let H, I be subgroups of G. Prove that one has $G/H \cong_G G/I$ if and only if the subgroups

H and I are conjugate in G.

Exercise 11. (a) Let G be a group. A *G-torsor* is a G-set that is G-isomorphic to the G-set G, on which G acts by left multiplication. Prove: the group of G-automorphisms of any G-torsor is, as a group, isomorphic to G itself.
(b) Let G be a group, let H be a subgroup of G, and let X be the G-set G/H, as defined in Exercise 10. Prove that that there is a group isomorphism $\mathrm{Aut}_G X \cong N_G(H)/H$; here $N_G(H)$ denotes the *normalizer* of H in G, which is defined by

$$N_G(H) = \{\sigma \in G : \sigma H \sigma^{-1} = H\}$$

(this is the largest subgroup of G in which H is normal).

Orbits. Let G be a group acting on a set X. We call x, $y \in X$ *equivalent under* G if there exists $\sigma \in G$ with $\sigma x = y$. One readily verifies that this is indeed an equivalence relation. The equivalence classes are called the *orbits* of X under G, and the orbit containing a given element x of X is denoted by Gx; so $Gx = \{\sigma x : \sigma \in G\}$. The set or equivalence classes, also called the *orbit space*, is denoted by $G\backslash X$; in the case of a right action, one writes X/G.

Exercise 12. Let G be a group acting on a set X, and let $x \in X$. The *stabilizer* or *decomposition group* of x in G is defined by $G_x = \{\sigma \in G : \sigma x = x\}$. Prove that G_x is a subgroup of G, and that there is an injective G-map $G/G_x \to X$ with image equal to Gx.

Exercise 13. Let G be a group acting on a set X. We call the action of G on X, or the G-set X, *transitive* if $\#(G\backslash X) = 1$. Prove that the following conditions are equivalent:
(i) the G-set X is transitive;
(ii) there exists a subgroup H of G with $X \cong_G G/H$;
(iii) $X \neq \emptyset$ and for all x, $y \in X$ there exists $\sigma \in G$ with $\sigma x = y$;
(iv) $X \neq \emptyset$, and any injective G-map $Y \to X$ from a non-empty G-set Y to X is a G-isomorphism.

Exercise 14. Let G be a group, let $H \subset G$ be a subgroup, and let X be the G-set G/H, as in Exercise 10. Prove that the kernel of the group homomorphism $G \to \mathrm{Sym}\, X$ that defines the action equals $\bigcap_{\sigma \in G} \sigma H \sigma^{-1}$.

Exercise 15. (a) Let G be a finite group, $H \subset G$ a subgroup, and write $n = (G : H)$. Suppose $\gcd\big((n-1)!, \#H\big) = 1$. Prove that H is normal in G.
(b) A group A is called *divisible* if for each $m \in \mathbf{Z}_{>0}$ and each $a \in A$ there exists $b \in A$ with $b^m = a$. Prove: if G is a group, and $H \subset G$ is a divisible subgroup of finite index, then H is normal in G.

Exercise 16. Let G be a group, let $H \subset G$ be a subgroup of finite index n, and suppose that $m \in \mathbf{Z}_{>0}$ is such that for each $\tau \in H$ one has $\tau^m = 1$. Prove that for all $\sigma \in G$ one has $\sigma^{nm} = 1$.

Exercise 17. (a) Let G be a group and $H \subset G$ a subgroup with $H \neq G$. Construct a G-set X and an element $\psi \in \operatorname{Sym} X$ such that $\psi \in \operatorname{Aut}_H X$ but $\psi \notin \operatorname{Aut}_G X$.
(b) Let $f\colon G_0 \to G_1$ be a group homomorphism. Prove: f is surjective if and only if for every group G_2 and any two group homomorphisms $g, h\colon G_1 \to G_2$ with $gf = hf$ one has $g = h$.

Exercise 18. Let G be a group, and let $H \subset G$ be a subgroup. We call H *maximal* if there are exactly 2 subgroups $J \subset G$ with $H \subset J$ (namely, $J = H$ and $J = G$).
(a) Prove: if $(G : H)$ is a prime number, then H is maximal.
(b) Prove: if H is maximal and normal, then $(G : H)$ is a prime number (and in particular finite).
(c) Prove: if G is finite with $\#G > 1$, and $(G : H)$ is the smallest prime number dividing $\#G$, then H is normal in G.
(d) Let p be a prime number. A *p-group* is a finite groups of which the order is of the form p^k, with $k \in \mathbf{Z}_{\geq 0}$. Prove: if G is a p-group and H is a maximal subgroup of G, then $(G : H) = p$ and H is normal in G.

Exercise 19. Let G be a group acting on a set X. An equivalence relation $\sim$ on X is called *G-invariant* if for any $\sigma \in G$ and any two $x, y \in X$ with $x \sim y$ one has $\sigma x \sim \sigma y$. The action of G on X, or the G-set X, is called *primitive*, if it is transitive and the number of G-invariant equivalence relations on X equals 2. Prove that the following conditions are equivalent:
(i) the G-set X is primitive;
(ii) there exists a maximal subgroup H of G (see Exercise 18) with $X \cong_G G/H$;
(iii) $\#X > 1$, the G-set X is transitive, and any surjective G-map $X \to Y$ from X to a G-set Y with $\#Y > 1$ is a G-isomorphism.

Exercise 20. Let G be a group acting on a set X. The action, or the G-set, is called *trivial* if for all $\sigma \in G$, $x \in X$ one has $\sigma x = x$.
Suppose that the number of G-invariant equivalence relations on X equals 2 but that the action is not primitive. Prove: $\#X = 2$, and the action is trivial.

Exercise 21. An action of a group G on a set X, or the G-set X, is called *faithful* if the group homomorphism $\phi\colon G \to \operatorname{Sym} X$ defining the action is injective.
Suppose G is an abelian group and that X is a faithful transitive G-set. Prove that X is a G-torsor, as defined in Exercise 11(a), and that $\#G = \#X$.

Exercise 22. Let k be a finite field, with prime field k_0, and denote by $\operatorname{Sym} k$ the group of permutations of the underlying set of k. Let G be the set of all $\sigma \in \operatorname{Sym} k$ for which there exist $a \in k^*$, $\phi \in \operatorname{Aut} k$, and $b \in k$ such that for all $x \in k$ one has $\sigma(x) = a \cdot \phi(x) + b$.
(a) Prove that G is a solvable subgroup of $\operatorname{Sym} k$ of order $\#k \cdot (\#k - 1) \cdot [k : k_0]$, and that the action of G on the underlying set of k is primitive and faithful.
(b) Prove: $G = \operatorname{Sym} k$ if and only if $\#k \leq 4$.

Exercise 23. Determine for each finite field k the least $t \in \mathbf{Z}_{\geq 0}$ for which the group G defined in Exercise 22 satisfies $G^{(t)} = \{1\}$; here the notation is as introduced before Exercise 1.

Exercise 24. Let $t \in \mathbf{Z}_{>0}$, let S be a set with $\#S = 2$, and put $X = S^t$. For $x = (x_i)_{i=0}^{t-1} \in X$ and $y = (y_i)_{i=0}^{t-1} \in X$, we define $d(x, y) = \min\{h \in \mathbf{Z}_{\geq 0} : x_i = y_i \text{ for all } i \geq h\}$. (This is a metric on X.) Put $G = \{\sigma \in \operatorname{Sym} X : d(\sigma x, \sigma y) = d(x, y) \text{ for all } x, y \in X\}$. Prove that G is a solvable group that acts faithfully and transitively on X, and that $\#G = 2^{\#X-1}$. For which t is the action primitive?

Exercise 25. Let G be a group acting faithfully on a set X. A *base* for the action is a subset $Y \subset X$ with the property that for each $\sigma \in G\backslash\{1\}$ there exists $y \in Y$ with $\sigma y \neq y$. Prove: if Y is a base for X, then $\#G \leq (\#X)^{\#Y}$.

Exercise 26. This exercise gives a categorical version of the main theorem of Galois theory. It is meant for students who are familiar, or willing to familiarize themselves, with the categorical terminology employed.
Let $K \subset L$ be a finite Galois extension of fields, and put $G = \operatorname{Gal}(L/K)$. Write $\mathcal{C}$ for the category of field extensions E of K that are K-isomorphic to some intermediate field of $K \subset L$, the morphisms in $\mathcal{C}$ being field homomorphisms that are the identity on K. Write $\mathcal{D}$ for the category of transitive G-sets, the morphisms being the G-maps.
(a) Let $F\colon \mathcal{C} \to \mathcal{D}$ send an object E of $\mathcal{C}$ to the set X_E of $\mathcal{C}$-morphisms $E \to L$, on which G acts by $\sigma f = \sigma \circ f$ (for $\sigma \in G$ and $f \in X_E$). Prove that F extends to a contravariant functor $\mathcal{C} \to \mathcal{D}$, and that for each E one has $\#X_E = [E : K]$.
(b) Show that, for each object X of $\mathcal{D}$, the set $J(X)$ of G-maps $X \to L$ can be viewed as an object of $\mathcal{C}$, and that J extends to a contravariant functor $\mathcal{D} \to \mathcal{C}$.
(c) Exhibit isomorphisms $\mathrm{id}_{\mathcal{C}} \to J \circ F$ and $\mathrm{id}_{\mathcal{D}} \to F \circ J$ of functors, and conclude that the categories $\mathcal{C}$ and $\mathcal{D}$ are anti-equivalent.

Exercise 27. Let $n \in \mathbf{Z}_{>0}$, let X be a set with $\#X = n$, and let $H \subset \operatorname{Sym} X$ be the subgroup generated by some n-cycle. Let $N_{\operatorname{Sym} X}(H)$ be as defined in Exercise 11(b). Prove: $N_{\operatorname{Sym} X}(H)/H \cong (\mathbf{Z}/n\mathbf{Z})^*$ (as groups).

Exercise 28. Let p be a prime number, let X be a set with $\#X = p$, and let G be a group acting faithfully and transitively on X. Prove: G is solvable if and only if $\#G < p^2$, and if and only if X has a base Y with $\#Y = 2$, and if and only if every subset $Y \subset X$ with $\#Y = 2$ is a base. (See Exercise 25 for the definition of a base.)

Exercise 29. Let K be a field of characteristic 0, let $f \in K[X]$ be an irreducible polynomial of prime degree p, and let L be a splitting field of f over K. Prove: L is solvable by radicals over K if and only if $[L : K] < p^2$, and if and only if there are α, $\beta \in L$ with $f(\alpha) = f(\beta) = 0$ and $L = K(\alpha, \beta)$, and if and only if for any α, $\beta \in L$ with $f(\alpha) = f(\beta) = 0$ and $\alpha \neq \beta$ one has $L = K(\alpha, \beta)$.

Extensions. Let A, C be groups. By an *extension* of C by A we mean a short exact sequence $1 \to A \to B \to C \to 1$ of groups. If

$$1 \to A \xrightarrow{f} B \xrightarrow{g} C \to 1, \qquad 1 \to A \xrightarrow{h} B' \xrightarrow{i} C \to 1$$

are two such extensions, then by a *morphism* from the first extension to the second we mean a group homomorphism $\psi\colon B \to B'$ such that $h = \psi f$ and $g = i\psi$.

Exercise 30. Let A, C be groups. Prove: any morphism between extensions as above is an *isomorphism* in the sense that it has a two-sided inverse that is also a morphism.

Exercise 31. In the terminology of the previous exercise, we call two extensions of C by A *isomorphic* if there is a morphism between them.
Suppose that each of A and C has order 2 or 3. In each of the four cases, determine the number of isomorphism classes of extensions of C by A.

G-groups. Let G be a group. By a *G-group* we mean a group A equipped with an action $G \times A \to A$, $(\sigma, \alpha) \mapsto {}^{\sigma}\alpha$, of G on the underlying set of A, such that for all $\sigma \in G$, α, $\beta \in A$ one has ${}^{\sigma}(\alpha\beta) = {}^{\sigma}\alpha \cdot {}^{\sigma}\beta$; equivalently, it is a group homomorphism $\phi\colon G \to \operatorname{Aut} A$, the connection between the two definitions being given by the formula ${}^{\sigma}\alpha = \phi(\sigma)(\alpha)$.

Exercise 32. Let G be a group and let A be a G-group. The *semidirect product* $A \rtimes G$, also written $A \rtimes_{\phi} G$ if ϕ defines the action of G on A, is the set $A \times G$ with multiplication $\cdot$ defined by $(\alpha, \sigma) \cdot (\beta, \tau) = (\alpha \cdot {}^{\sigma}\beta, \sigma\tau)$, for α, $\beta \in A$, σ, $\tau \in G$.
Prove that $A \rtimes G$ is a group with this multiplication, and that there is a short exact sequence $1 \to A \xrightarrow{f} A \rtimes G \xrightarrow{g} G \to 1$, where $f(\alpha) = (\alpha, 1)$ and $g(\alpha, \sigma) = \sigma$, for $\alpha \in A$, $\sigma \in G$.

Exercise 33. Let $1 \to A \to B \to G \to 1$ be a short exact sequence of groups. It is said to *split* if there is a group homomorphism $B \to A$ such that the composed map $A \to B \to A$ equals the identity on A, and it is said to be *semi-split* if there is a group homomorphism $G \to B$ such that the composed map $G \to B \to G$ is the identity on G. (*Note*: this terminology is not completely standard; sometimes the two notions are confused.)
(a) Prove: the sequence splits if and only if, as an extension of G by A, it is isomorphic (in the sense of Exercise 31) to the sequence $1 \to A \xrightarrow{f} A \times G \xrightarrow{g} G \to 1$, where $f(\alpha) = (\alpha, 1)$ and $g(\alpha, \sigma) = \sigma$, for $\alpha \in A$, $\sigma \in G$.
(b) Prove: the sequence is semi-split if and only if there is a G-group structure on A such that the sequence is isomorphic to the sequence containing the semidirect product that occurs in Exercise 32.
(c) Prove: if B is abelian, or more generally the image of A is contained in the center of B, then the sequence splits if and only if it is semi-split.

Exercise 34. Let G be a group and let A be a G-group. Prove that $A \rtimes G$ acts on the underlying set of A by the formula $(\alpha, \sigma)\beta = \alpha \cdot {}^{\sigma}\beta$, that this action is transitive, and that

the stabilizer of $1 \in A$ in $A \rtimes G$ is the subgroup $\{1\} \rtimes G$ of $A \rtimes G$.

Exercise 35. Let G_0, G_1, G_2 be groups, and let for each i, $j \in \mathbf{Z}$ with $0 \leq i < j \leq 2$ the group G_j have the structure of a G_i-group. Suppose moreover that these three actions are compatible in the sense that for all $\alpha \in G_0$, $\beta \in G_1$, $\gamma \in G_2$ one has ${}^{\alpha}({}^{\beta}\gamma) = {}^{({}^{\alpha}\beta)}({}^{\alpha}\gamma)$. Show that one can make $G_2 \rtimes G_1$ into a G_0-group and G_2 into a $G_1 \rtimes G_0$-group such that there is a group isomorphism $(G_2 \rtimes G_1) \rtimes G_0 \cong G_2 \rtimes (G_1 \rtimes G_0)$.
Note. This group will be denoted $G_2 \rtimes G_1 \rtimes G_0$.

Exercise 36. Let k be a finite field, and define G_0, G_1, and G_2 to be the automorphism group $\operatorname{Aut} k$, the multiplicative group $k^* = k\backslash\{0\}$, and the additive group k^+ of k, respectively. Define actions as in Exercise 35 such that the group $G_2 \rtimes G_1 \rtimes G_0$ becomes isomorphic to the group G occurring in Exercise 22.

Exercise 37. (a) Formulate conditions for groups G_0, G_1, ..., G_n under which one can meaningfully define a group $G_n \rtimes \ldots \rtimes G_1 \rtimes G_0$, generalizing the case $n = 2$ from Exercise 35. (You will get extra credit for this exercise if you have a particularly clean proof that your conditions are sufficient.)
(b) Let $t \in \mathbf{Z}_{>0}$ and put $G_i = (\mathbf{Z}/2\mathbf{Z})^{2^i}$ for $0 \leq i \leq t-1$. Prove that for suitable actions (satisfying your conditions from (a)), the group G from Exercise 24 is isomorphic to $G_{t-1} \rtimes \ldots \rtimes G_1 \rtimes G_0$.

Exercise 38. Let G be a group. Make G into a G-group by letting it act upon itself by conjugation: ${}^{\sigma}\tau = \sigma\tau\sigma^{-1}$ for σ, $\tau \in G$. Prove: $G \rtimes G \cong G \times G$.

Exercise 39. (a) Let $n \in \mathbf{Z}_{>0}$, and let $1 \to A_1 \to A_2 \to \ldots \to A_n \to 1$ be an exact sequence of groups. Suppose that all A_i with at most one exception are finite. Prove that they are all finite, and that one has $\prod_{i=1}^{n} (\#A_i)^{(-1)^i} = 1$.
(b) Let $n \in \mathbf{Z}_{>0}$, and let $A_0 \to A_1 \to \ldots \to A_n \to A_0$ be an exact sequence of groups such that the kernel of the first map equals the image of the last. Suppose that all A_i with at most one exception are finite. Prove that they are all finite, that $\prod_{i=0}^{n} \#A_i$ is the square of some integer, and that for odd n one has $\prod_{i=0}^{n} (\#A_i)^{(-1)^i} = 1$.

Exercise 40. A *minimal normal* subgroup of a group G is a normal subgroup N of G such that there are precisely 2 normal subgroups of G that are contained in N, namely $\{1\}$ and N.
Let G be a finite solvable group acting faithfully and primitively on some set. In class we proved that G has exactly one minimal normal subgroup N, and that N is also the only non-trivial abelian normal subgroup of G. Prove that there is a unique non-negative integer l with $N = G^{(l)}$.

Exercise 41. Let G be a group and let A be a G-group. By a *G-subgroup* of A we mean a subgroup B of A such that for all $\sigma \in G$ and $\beta \in B$ one has ${}^{\sigma}\beta \in B$.
(a) Exhibit a bijection between the set of G-subgroups of A and the set of subgroups

$H \subset A \rtimes G$ with $\{1\} \rtimes G \subset H$.
(b) Let $A \rtimes G$ act on the underlying set of A as in Exercise 34(b). Prove that this action is primitive if and only if A has precisely two G-subgroups.

Exercise 42. Let A, B, C be groups. A map $f\colon A \times B \to C$ is called *bilinear* if for all α, $\alpha' \in A$ and β, $\beta' \in B$ one has $f(\alpha\alpha', \beta) = f(\alpha, \beta)\cdot f(\alpha', \beta)$ and $f(\alpha, \beta\beta') = f(\alpha, \beta)\cdot f(\alpha, \beta')$.
(a) Suppose $f\colon A\times B \to C$ is bilinear. Prove that the subgroup of C generated by $f(A\times B)$ is abelian.
(b) Exhibit a bijection between the set of bilinear maps $A \times B \to C$ and the set of group homomorphisms $(A/[A, A]) \otimes_{\mathbf{Z}} (B/[B, B]) \to C$.

Exercise 43. Let A and B be subgroups of a group G. Prove that the map $A \times B \to G$ sending (α, β) to the *commutator* $[\alpha, \beta] = \alpha\beta\alpha^{-1}\beta^{-1}$ is bilinear (as defined in Exercise 42) if and only if the image of this map is contained in the center of the subgroup of G generated by A and B.

Exercise 44. (a) Let G be a group that has at most one non-trivial abelian normal subgroup. Prove that the center of G is either trivial (i.e., equal to $\{1\}$) or finite of prime order.
(b) Let G be a finite solvable group acting faithfully and primitively on a set X. Prove that the center of G is non-trivial if and only if there exists a prime number p such that $\#G = \#X = p$.

Exercise 45. Let R be a ring and let S be a set. The *support* of a map $f\colon S \to R$ is the subset $\operatorname{supp} f = \{s \in S : f(s) \neq 0\}$ of S, and a map $f\colon S \to R$ is said to be *of finite support* if $\#\operatorname{supp} f < \infty$. We write R^S for the set of all maps $S \to R$, and $R^{(S)}$ for the set of all maps $S \to R$ of finite support.
(a) Prove that R^S has exactly one R-module structure with the property that for each $s \in S$ the map $R^S \to R$, $f \mapsto f(s)$, is R-linear.
(b) Prove that $R^{(S)}$ is a sub-R-module of R^S.

Exercise 46. Let R be a ring, S a set, and $R^{(S)}$ the R-module from Exercise 45. Exhibit, for each R-module M, a bijection between the set of all maps $S \to M$ and the set of all R-linear maps $R^{(S)} \to M$.

Exercise 47. Let R be a ring. An R-module F is called *free* if there is a set S such that F is isomorphic, as an R-module, to the module $R^{(S)}$ from Exercise 45.
(a) Suppose R is a field. Prove: every R-module is free. Can you prove the same statement if R is only assumed to be a division ring? (A *division ring* is a ring R for which the unit group R^* equals $R\backslash\{0\}$.)
(b) Let $0 \to L \to M \to N \to 0$ be an exact sequence of R-modules, with N free. Prove: the sequence splits.

Exercise 48. Let R be a ring, let K, L, M, N be R-modules, and let $f\colon K \to L$,

$g\colon L \to M$, $h\colon M \to N$ be R-linear maps such that $h \circ g \circ f = 0$ (the zero map). Construct an exact sequence
of R-modules, where ker denotes kernel, im denotes image, and cok denotes cokernel.
This result is often called the *snake lemma*. Can you see why?

Exercise 49. Let $G = \{1, \sigma\}$ be a multiplicatively written group of order 2, and let M be a finite additively written G-module for which $\#M$ is odd. Prove that $M^+ = \{x \in M : \sigma x = x\}$ and $M^- = \{x \in M : \sigma x = -x\}$ are sub-G-modules of M and that there is an isomorphism $M \cong M^+ \oplus M^-$ of G-modules.

Exercise 50. Let G be a group of order 2. Prove that each simple G-module is finite of prime order, and that conversely for each prime number p there are, up to isomorphism, exactly two simple G-modules if p is odd and exactly one if $p = 2$.

Exercise 51. Let R be a ring and M an R-module. An R-linear map $M \to M$ is called an *endomorphism* (or R-*endomorphism*) of M. We write $\mathrm{End}M$ for the set of all endomorphisms of M.
(a) Prove that $\mathrm{End}M$ is a ring with pointwise addition (i.e., $(f+g)(x) = f(x) + g(x)$ for all $f, g \in \mathrm{End}M$, $x \in M$) and composition as multiplication.
(b) Let S be a set with $\#S = n < \infty$, and suppose $M = R^{(S)}$ as in Exercise 45. Prove that $\mathrm{End}M$ is, as a ring, isomorphic to the ring $M_n(R^{\mathrm{opp}})$ of $n \times n$-matrices over the ring R^{opp} from Exercise 8.

Exercise 52. Let R be a ring and let M be a simple R-module. Prove that the ring $\mathrm{End}M$ from Exercise 51 is a division ring (see Exercise 47(a)).

Exercise 53. Let k be a field and $M_2(k)$ the ring of 2×2-matrices over k. We view the k-vector space k^2 as a module over $M_2(k)$ by writing the elements of k^2 as column vectors and defining $A \cdot v$ as the usual product Av, for $A \in M_2(k)$, $v \in k^2$.
(a) Prove that k^2 is a simple $M_2(k)$-module.
(b) According to (a) and Exercise 52, the ring $\mathrm{End}(k^2)$ of $M_2(k)$-endomorphisms of k^2 is a division ring. Which division ring is it?

Exercise 54. In class it is proved that a module M over a ring R is simple if and only if there is a maximal left ideal $\mathfrak{m}$ of R such that $M \cong R/\mathfrak{m}$ (as R-modules).
Suppose now that R is a *commutative* ring and that M is a simple R-module. Prove that there is a *unique* maximal ideal $\mathfrak{m}$ of R such that $M \cong R/\mathfrak{m}$ (as R-modules), and that the division ring $\mathrm{End}M$ from Exercise 52 is a field.

Exercise 55. Give an example of a ring R and a simple R-module M with the property that the division ring $\mathrm{End}M$ from Exercise 52 is not a field.

Exercise 56. Let n be an integer, A an additively written abelian group, and $n_A\colon A \to A$ the map $a \mapsto na$. Prove: $(\mathbf{Z}/n\mathbf{Z}) \otimes_{\mathbf{Z}} A \cong \mathrm{cok}\, n_A$.

Exercise 57. A *torsion* group is a group of which every element has finite order. Prove: if A and B are abelian groups such that A is torsion and B is divisible (see Exercise 15(b)), then $A \otimes_{\mathbf{Z}} B = 0$.

Exercise 58. Describe the group $A \otimes_{\mathbf{Z}} B$ when each of A and B is one of the following: (a) finite cyclic; (b) infinite cyclic; (c) the Klein four group; (d) the additive group $\mathbf{Q}$; and (e) $\mathbf{Q}/\mathbf{Z}$. (Be sure to cover all combinations.)

Exercise 59. Construct a non-trivial abelian group A such that $A \otimes_{\mathbf{Z}} A = 0$. Can such a group be finitely generated?

Exercise 60. Let A, B, C be additively written abelian groups, and let $f\colon A \times B \to C$ be a bilinear map that is also a group homomorphism. Prove that f is the zero map.

Exercise 61. In this exercise, all tensor products are over $\mathbf{Z}$.
Is the tensor product of two finitely generated abelian groups finitely generated? Is the tensor product of two finite abelian groups finite? Give in each case a proof or a counterexample.

Exercise 62. Suppose that A and B are non-zero finitely generated abelian groups. Prove: $A \otimes_{\mathbf{Z}} B = 0$ if and only if A and B are finite with $\gcd(\#A, \#B) = 1$.

Exercise 63. Let k be a field, let V be the k-vector space k^2, and let $M_2(k)$ be the ring of 2×2-matrices over k. We view $M_2(k)$ as a k-vector space in the natural way. Define the map $f\colon V \times V \to M_2(k)$ by $f\big((a,b),(c,d)\big) = \left(\begin{smallmatrix} ac & ad \\ bc & bd \end{smallmatrix}\right)$.
(a) Prove that f is k-bilinear, and that the image of f consists of the set of 2×2-matrices over k of rank at most 1.
(b) Prove that the pair $\big(M_2(k), f\big)$ is a tensor product of V and V over k, as defined in class.
(c) Prove that not every element of $V \otimes_k V$ is of the form $x \otimes y$, with x, $y \in V$.

Exercise 64. Let A and B be abelian groups.
(a) Prove: if at least one of A and B is cyclic, then every element of $A \otimes_{\mathbf{Z}} B$ is of the form $x \otimes y$, with $x \in A$, $y \in B$.
(b) Suppose A is finitely generated. Prove: A is cyclic if and only if every element of $A \otimes_{\mathbf{Z}} A$ is of the form $x \otimes y$, with x, $y \in A$.

Exercise 65. Let A be an additively written abelian group. For $n \in \mathbf{Z}$, we write $nA = \{nx : x \in A\}$. Let $a \in A$.
(a) Prove: the element $a \otimes a$ of $A \otimes_{\mathbf{Z}} A$ equals 0 if there exists $n \in \mathbf{Z}$ with $na = 0$ and $a \in nA$.
(b) Is the statement in (a) valid with "if" replaced by "only if"? Give a proof or a counterexample.

Exercise 66. A partially ordered set $(I, \leq)$ is called *directed* if for any i, $j \in I$ there exists $k \in I$ such that $i \leq k$ and $j \leq k$. An *injective system* of groups is a system $(A_i)_{i \in I}$ of groups, where I is a non-empty directed partially ordered set, together with a system of group homomorphisms $f_{ij} \colon A_i \to A_j$, one for each pair $(i, j) \in I \times I$ with $i \leq j$, such that for each $i \in I$ the map f_{ii} is the identity map on A_i, and such that for any triple $(i, j, k) \in I \times I \times I$ with $i \leq j \leq k$ one has $f_{ik} = f_{jk} \circ f_{ij}$. Let such a system be given. Call an element $a \in A_i$ *equivalent* to an element $b \in A_j$ if there exists $k \in I$ with $i \leq k$, $j \leq k$, and $f_{ik}(a) = f_{jk}(b)$.
(a) Prove that this does define an equivalence relation on the disjoint union of the groups A_i.
(b) The set of equivalence classes of the equivalence relation is called the *injective limit* of the system, notation: $\varinjlim A_i$. Prove that $\varinjlim A_i$ has a unique group structure with the property that for each $j \in I$, the map $A_j \to \varinjlim A_i$ sending each $a \in A_j$ to the equivalence class containing a is a group homomorphism.

Exercise 67. (a) Prove that any group is isomorphic to the injective limit of a system of *finitely generated* groups.
(b) A group is said to be *finitely presented* if it can be defined with a finite number of generators and a finite number of relations. Prove that any group is isomorphic to the injective limit of a system of finitely presented groups.

Exercise 68. Let R be a ring, and let $(B_i)_{i \in I}$ be an injective system of R-modules such that all maps f_{ij} are R-linear.
(a) Prove that the group $\varinjlim B_i$ has a unique R-module structure such that for each $j \in I$ the natural map $B_j \to \varinjlim B_i$ is R-linear.
(b) Let A be a right R-module. Prove that $(A \otimes_R B_i)_{i \in I}$, with the maps $\mathrm{id}_A \otimes f_{ij}$, is an injective system of abelian groups, and that there is an isomorphism $A \otimes_R (\varinjlim B_i) \cong \varinjlim (A \otimes_R B_i)$ of abelian groups.

Exercise 69. Let R be a ring, let $0 \to L \to M \to N \to 0$ be an exact sequence of right R-modules, and let B be a left R-module. Prove that the induced sequence $0 \to L \otimes_R B \to M \otimes_R B \to N \otimes_R B \to 0$ is exact if B is free, and also if R is a field. Give an example in which it is not exact.

Exercise 70. An abelian group A is called *torsionfree* if it has no nontrivial elements of finite order. Let A be a torsionfree abelian group, and let $0 \to B \to C \to D \to 0$ be an exact sequence of abelian groups. Prove: the sequence $0 \to A \otimes B \to A \otimes C \to A \otimes D \to 0$ is exact, all tensor products being taken over $\mathbf{Z}$.

Exercise 71. Let G be a group, $H \subset G$ a subgroup, and M an H-module. In class we defined the G-module *induced* from M to be the $\mathbf{Z}[G]$-module $\mathbf{Z}[G] \otimes_{\mathbf{Z}[H]} M$, where $\mathbf{Z}[G]$ is viewed as a $\mathbf{Z}[G]$-$\mathbf{Z}[H]$-bimodule. One can also define the G-module that is *co-induced* from M; it is the $\mathbf{Z}[G]$-module $\mathrm{Hom}(\mathbf{Z}[G], M)$ consisting of all $\mathbf{Z}[H]$-linear maps

$\mathbf{Z}[G] \to M$, where now $\mathbf{Z}[G]$ is viewed as a $\mathbf{Z}[H]$-$\mathbf{Z}[G]$-bimodule, and the $\mathbf{Z}[G]$-module structure is defined by $(rf)(x) = f(xr)$, for $r, x \in \mathbf{Z}[G]$ and $f \in \mathrm{Hom}(\mathbf{Z}[G], M)$.
(a) Prove that this indeed defines a $\mathbf{Z}[G]$-module structure on $\mathrm{Hom}(\mathbf{Z}[G], M)$.
(b) Exhibit an injective $\mathbf{Z}[G]$-linear map $\mathbf{Z}[G] \otimes_{\mathbf{Z}[H]} M \to \mathrm{Hom}(\mathbf{Z}[G], M)$ that is an isomorphism in the case $(G : H) < \infty$.

Exercise 72. Let G be a finite solvable group acting faithfully and primitively on some set. Let N be a non-trivial abelian normal subgroup of G. Prove that the number of normal subgroups of G is exactly 1 more than the number of normal subgroups of G/N.

Exercise 73. Let R be a ring, and let

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$$

be an exact sequence of R-modules. Prove that the set of all R-linear automorphisms ψ of M with $f = \psi f$ and $g = g\psi$ is a subgroup of the group of all R-linear automorphisms of M, and that this subgroup is isomorphic to the group of all R-linear maps $N \to L$.

Exercise 74. Let D_4 be the dihedral group of order 8. View $\mathbf{R}^2$ as a faithful D_4-module in the usual way. Prove that $\mathbf{R}^2$ is induced from some subgroup of D_4 of index 2.

Exercise 75. Let k be a field, and let $n \in \mathbf{Z}_{>0}$. Let G be the set of all non-singular $n \times n$-matrices M over k with the property that each column of M has exactly one non-zero entry (such matrices are often called *monomial*). Write $X = \{1, 2, \ldots, n\}$ and $S_n = \mathrm{Sym}\, X$. Prove that G is a group, and that G is isomorphic to the wreath product $k^* \wr_X S_n$.

Exercise 76. Let G be a group and let R be a ring. Show that the group ring $R[G]$ can in a natural way be made into a G-module, and that this G-module is induced from the trivial subgroup $\{1\}$ of G.

In Exercises 77–81, we let G and H be groups, X is a G-set, and the wreath product $H \wr_X G$ is as defined in class.

Exercise 77. Suppose $\#H = \#G = \#X = 2$. To which well-known group is $H \wr_X G$ isomorphic if the action of G on X is non-trivial? and if it is trivial?

Exercise 78. Let Y be an H-set. In class we defined an action of $H \wr_X G$ on $Y \times X$. Prove: this action is transitive if and only if X is a transitive G-set and Y is a transitive H-set.

Exercise 79. Let the notation be as in Exercise 78. Give necessary and sufficient conditions for the action of $H \wr_X G$ on $Y \times X$ to be primitive, and for this action to be faithful.

Exercise 80. Suppose $\#H = 2$ and $\#G = \#X = 3$, the action of G on X being non-

trivial. Prove that $H \wr_X G$ is isomorphic to the product of a group of order two and the alternating group A_4.

Exercise 81. Suppose X is finite and non-empty. Exhibit a surjective group homomorphism $H \wr_X G \to H/[H,H]$.

Exercise 82. Let X be a finite set. An element of $\operatorname{Sym} X$ is called a *transposition* if it interchanges two elements of X and is the identity on the rest. Let $G \subset \operatorname{Sym} X$ be a subgroup, let $\mathcal{T} \subset G$ be the set of transpositions in G, and let $H \subset G$ be the subgroup generated by $\mathcal{T}$. For $x,\ y \in X$, we write $x \sim y$ if there exists an element of $\mathcal{T}$ that interchanges x and y.
(a) Prove that $\sim$ is a G-invariant equivalence relation on X, and that the equivalence classes of $\sim$ coincide with the orbits of X under H.
(b) Prove: $H = \{\sigma \in \operatorname{Sym} X : \text{for all } x \in X \text{ one has } x \sim \sigma x\}$, and H is normal in G.
(c) Suppose G is transitive on X. Denote by $X/\!\sim$ the set of equivalence classes of $\sim$. Prove that all equivalence classes of $\sim$ have the same number m of elements, and that there is a subgroup J of $\operatorname{Sym}(X/\!\sim)$ such that G is isomorphic to the wreath product $S_m \wr J$ with respect to $X/\!\sim$.

Exercise 83. Let A be an abelian group A. We write A_{tor} for the set of elements of A of finite order.
(a) Prove that A_{tor} is a subgroup of A, and that it is the kernel of the group homomorphism $A \to A \otimes_{\mathbf{Z}} \mathbf{Q}$ sending a to $a \otimes 1$.
(b) Prove that there is an exact sequence

$$0 \to A_{\mathrm{tor}} \to A \to A \otimes_{\mathbf{Z}} \mathbf{Q} \to A \otimes_{\mathbf{Z}} (\mathbf{Q}/\mathbf{Z}) \to 0$$

of abelian groups.

Exercise 84. In this exercise, all tensor products are over $\mathbf{Z}$.
Let $0 \to A \to B \to C \to 0$ be an exact sequence of abelian groups. Show that the induced sequence

$$0 \to A \otimes \mathbf{Q} \to B \otimes \mathbf{Q} \to C \otimes \mathbf{Q} \to 0$$

is exact, and exhibit an exact sequence

$$0 \to A_{\mathrm{tor}} \to B_{\mathrm{tor}} \to C_{\mathrm{tor}} \to A \otimes (\mathbf{Q}/\mathbf{Z}) \to B \otimes (\mathbf{Q}/\mathbf{Z}) \to C \otimes (\mathbf{Q}/\mathbf{Z}) \to 0$$

of abelian groups, the notation $-_{\mathrm{tor}}$ being as in Exercise 83.

Exercise 85. (a) For a finite separable field extension $K \subset L$, with normal closure N, we write $G_{L/K}$ for the Galois group of N over K, and $X_{L/K}$ for the set of field homomorphisms $L \to N$ that are the identity on K.
(a) Let $K \subset L$ be a finite separable field extension. Exhibit a faithful transitive action of $G_{L/K}$ on $X_{L/K}$.

(b) Let $K \subset L \subset M$ be finite separable field extensions, and put $X = X_{L/K}$. Prove that $G_{M/K}$ is isomorphic to a subgroup of $G_{M/L} \wr_X G_{L/K}$.

The second exterior power. Let R be a commutative ring. The *second exterior power* $\bigwedge_R^2 M$ of an R-module M is defined to be the R-module $(M \otimes_R M)/N$, where N is the sub-R-module of $M \otimes_R M$ generated by $\{x \otimes x : x \in M\}$; for x, $y \in M$, the image of $x \otimes y$ in $\bigwedge_R^2 M$ is denoted by $x \wedge y$. If A is an abelian group, we write $\bigwedge^2 A$ for $\bigwedge_{\mathbf{Z}}^2 A$.

Exercise 86. Let R be a commutative ring.
(a) Let M, N be R-modules. Exhibit an isomorphism

$$\bigwedge_R^2 (M \oplus N) \cong \Big(\bigwedge_R^2 M\Big) \oplus \big(M \otimes_R N\big) \oplus \Big(\bigwedge_R^2 N\Big)$$

of R-modules.
(b) Let F be a free R-module with basis $(e_i)_{i\in I}$, and let $<$ be a total ordering on I. Prove that $\bigwedge_R^2 F$ is a free R-module with basis $(e_i \wedge e_j)_{i,j\in I, i<j}$.

Exercise 87. (a) Let G be a group with $[G,G] \subset Z(G)$. Prove that there is a group homomorphism $\bigwedge^2 \big(G/Z(G)\big) \to [G,G]$ sending $\big(aZ(G)\big) \wedge \big(bZ(G)\big)$ to $[a,b] = aba^{-1}b^{-1}$, for a, $b \in G$.
(b) Let A be a finite abelian group. Prove: the group $\bigwedge^2 A$ is cyclic of order 2 if and only if A is the direct sum of a group of order 2 and a finite cyclic group of even order.

Exercise 88. (a) Let F be a free abelian group with basis $(e_i)_{i\in I}$, and let $<$ be a total ordering on I. Let G be the set $\big(\bigwedge^2 F\big) \times F$. For $(x, \sum_{i\in I} n_i e_i)$, $(y, \sum_{i\in I} m_i e_i) \in G$ (with n_i, $m_i \in \mathbf{Z}$ for all $i \in I$, and $n_i = m_i = 0$ for almost all $i \in I$), define

$$\big(x, \textstyle\sum_{i\in I} n_i e_i\big) * \big(y, \sum_{i\in I} m_i e_i\big) = \big(x + y + \sum_{i,j\in I, i<j} n_i m_j e_i \wedge e_j, \sum_{i\in I}(n_i + m_i)e_i\big).$$

Prove that G is a group with the operation $*$, and that $[G,G] = \big(\bigwedge^2 F\big) \times \{0\}$.
(b) Let A, B be abelian groups, and let $f\colon \bigwedge^2 A \to B$ be a group homomorphism. Prove that there exists an exact sequence

$$1 \to B \xrightarrow{i} E \xrightarrow{p} A \to 1$$

of groups such that for all x, $y \in E$ one has $i \circ f\big(p(x) \wedge p(y)\big) = [x,y]$. (*Hint.* Do first the case A is free.)

Exercise 89. Let G and H be solvable groups. Prove that for every G-set X the wreath product $H \wr_X G$ is a solvable group.

Exercise 90. Let R be a commutative ring, M an R-module, and I an ideal of R. Write $M[I] = \{x \in M : rx = 0 \text{ for all } r \in I\}$.

(a) Prove that $M[I]$ is a sub-R-module of M, and that the R-module $M[I]$ may be viewed as an R/I-module.
(b) Exhibit a group isomorphism $M[I] \cong \mathrm{Hom}_R(R/I, M)$.

Exercise 91. Let R be a commutative ring.
(a) Let S be a finite set of maximal ideals of R. Prove that for every $\mathfrak{m} \in S$ there exists $e_\mathfrak{m} \in \bigcap_{\mathfrak{n}\in S, \mathfrak{n}\neq\mathfrak{m}} \mathfrak{n}$ with $e_\mathfrak{m} \equiv 1 \bmod \mathfrak{m}$.
(b) Let T be the set of all maximal ideals of R, and let the notation $M[\mathfrak{m}]$ be as in Exercise 90. Prove that the map $\bigoplus_{\mathfrak{m}\in T} M[\mathfrak{m}] \to M$ sending $(x_\mathfrak{m})_{\mathfrak{m}\in T}$ to $\sum_{\mathfrak{m}\in T} x_\mathfrak{m}$ is injective.

Exercise 92. In Exercise 67, a group G was said to be *finitely presented* if it can be defined with a finite number of generators and a finite number of relations; more formally, this means that there exist a finitely generated free group F, a surjective group homomorphism $f\colon F \to G$, and a finite subset $R \subset F$, such that the kernel of f is generated by the set of elements of F that are conjugate to an element of R.
Suppose that G is a finitely presented group, that F' is a finitely generated group, and that $f'\colon F' \to G$ is a surjective group homomorphism. Prove that there is a finite subset $R' \subset F'$ such that the kernel of f' is generated by the set of elements of F' that are conjugate to an element of R'.

Exercise 93. The purpose of this exercise, which counts for two, is to construct a finitely generated group that is not finitely presented.
(a) Suppose G is a group that is generated by 2 elements such that the center $Z(G)$ of G is not a finitely generated group. Prove: $G/Z(G)$ is a finitely generated group that is not finitely presented. (You may use the result of Exercise 92.)
(b) Let F be an additively written free abelian group with basis $(e_i)_{i\in\mathbf{Z}}$, and let $H \subset F$ be the subgroup generated by $\{e_h : h \in \mathbf{Z}_{>0}\}$. Let the bilinear map $f\colon F \times F \to H$ map (e_i, e_j) to e_{i-j} if $i > j$ and to 0 if $i \leq j$. Write Γ for the set $H \times F$, and define the operation $*$ on Γ by $(x, a) * (y, b) = (x + y + f(a, b), a + b)$. Prove that this is a group operation, that the group Γ satisfies $[\Gamma, \Gamma] = Z(\Gamma) = H \times \{0\}$, and that Γ has an automorphism σ that is the identity on $H \times \{0\}$ and maps each $(0, e_i)$ to $(0, e_{i+1})$.
(c) With Γ and σ as in (b), denote by $\langle\sigma\rangle$ the subgroup of $\mathrm{Aut}\,\Gamma$ generated by σ and by G the semidirect product $\Gamma \rtimes \langle\sigma\rangle$. Prove that $G/Z(G)$ is a finitely generated group that is not finitely presented.
(d) Show that $G/Z(G)$ is isomorphic to a subgroup of the wreath product $\mathbf{Z} \wr_X \langle\sigma\rangle$, where X is an infinite transitive $\langle\sigma\rangle$-set.

Exercise 94. The *exponent* of a finite group is the least common multiple of the orders of all of its elements.
Let G, A be finite groups with A cyclic. Prove: $\#\mathrm{Hom}(G, A) \leq \#G$, with equality if and only if G is abelian of exponent dividing $\#A$.

Exercise 95. Let G, A be finite groups with A cyclic, and suppose that one has $\#\mathrm{Hom}(G, A) =$

$\#G$. Prove that for each subgroup H of G there is an exact sequence

$$0 \to \mathrm{Hom}(G/H, A) \to \mathrm{Hom}(G, A) \to \mathrm{Hom}(H, A) \to 0$$

of abelian groups.

Exercise 96. Let k be a field, let $n \in \mathbf{Z}_{\geq 0}$, and let k^n be the standard k-vector space of dimension n. We write $M(n, k)$ for the ring of k-endomorphisms of k^n, and $\mathrm{GL}(n, k) = M(n, k)^*$ for the group of k-automorphisms of k^n; these may, respectively, be identified with the ring of $n \times n$-matrices over k and the group of invertible $n \times n$-matrices over k. The natural ring homomorphism $k \to M(n, k)$ induces a group homomorphism $k^* \to \mathrm{GL}(n, k)$, which we regard as an inclusion map if $n > 0$. The image of the map $k^* \to \mathrm{GL}(n, k)$ is normal, and the cokernel of the map is denoted by $\mathrm{PGL}(n, k)$.
(a) Write $\mathbf{P}^{n-1}(k)$ for the set of orbits of $k^n \backslash \{0\}$ under k^*. Exhibit a faithful action of $\mathrm{PGL}(n, k)$ on $\mathbf{P}^{n-1}(k)$.
(b) Let k be a finite field, and write $q = \#k$. Prove that $\mathrm{PGL}(2, k)$ is isomorphic to a subgroup of the symmetric group S_{q+1}. Which subgroup is this for $q = 2$, $q = 3$, $q = 4$?

Exercise 97. Let G be the group $\mathrm{GL}(2, \mathbf{F}_3)$. Prove that G is a finite solvable group, and that the natural action of G on $\mathbf{F}_3^2$ makes $\mathbf{F}_3^2$ into a primitive faithful G-module.

Exercise 98. Let $\mathbf{F}_9$ be a field with $\#\mathbf{F}_9 = 9$. Denote by H the subgroup of $\mathrm{GL}(2, \mathbf{F}_9)$ generated by $\mathbf{F}_9^*$ and $\mathrm{GL}(2, \mathbf{F}_3)$. Let Δ be the group of field automorphisms of $\mathbf{F}_9$ (so $\#\Delta = 2$). Put $G = H \rtimes \Delta$, with Δ acting entry-wise on H.
(a) Compute the orders of H and G, and prove that the natural action of H on $\mathbf{F}_9^2$ and the componentwise action of Δ on $\mathbf{F}_9^2$ combine into an action of G on $\mathbf{F}_9^2$, making $\mathbf{F}_9^2$ into a faithful G-module.
(b) Prove that the subring of $M(2, \mathbf{F}_9)$ generated by H equals $M(2, \mathbf{F}_9)$, and that $\mathbf{F}_9^2$ is simple both as an H-module and as a G-module.
(c) Can you prove that $\mathbf{F}_9^2$ is primitive both as an H-module and as a G-module? (This is not so easy. You will earn extra credit with a good solution.)

Exercise 99. Let W be the $\mathbf{F}_3$-vector space $\mathbf{F}_3^2$, and let V be the $\mathbf{F}_3$-vector space $W \otimes_{\mathbf{F}_3} W$. Let τ be the unique automorphism of V with $\tau(x \otimes y) = y \otimes x$ for all x, $y \in W$. Denote by G the subgroup of $\mathrm{Aut}\, V$ generated by τ and all maps of the form $\alpha \otimes \beta$, with α, $\beta \in \mathrm{Aut}\, W$.
(a) Prove that G is a solvable group of order 2304.
(b) Prove that V is a simple G-module.
(c) Can you prove that V is a primitive G-module? (This is again worth extra credit.)

Exercise 100. Suppose G is a finite solvable group for which there is a primitive faithful G-module. In class we considered a chain of normal subgroups $A \subset B \subset C$ of G, where A is a maximal abelian normal subgroup of G, the group C is the centralizer of A in G, and B is maximal among all normal subgroups H of G with $A \subset H \subset C$ and H/A abelian.

(a) Identify such groups A, B, C if G is the group from Exercise 98, and verify the statements, proved in class, that A is cyclic, that $\#(B/A)$ is a square, and that C/B is isomorphic to a subgroup of $\mathrm{Aut}(B/A)$.
(b) Same questions for the group G from Exercise 99.

Exercise 101. Let G be a finite solvable group with the property that each abelian normal subgroup of G is cyclic. Let the normal subgroups A, B, C of G be as in Exercise 100. In class we saw that there is a group isomorphism $B/A \to \mathrm{Hom}(B/A, A)$ sending the coset bA to the map $B/A \to A$ sending the coset cA to $bcb^{-1}c^{-1}$.
(a) Let $n \in \mathbf{Z}_{>0}$, and define $H \subset B$ by $H = \{b \in B : (bA)^n = 1 \text{ in } B/A, \text{ and } bA = (cA)^n \text{ for some } c \in B\}$. Prove that H is an abelian normal subgroup of G containing A, and conclude that one has $H = A$.
(b) An integer is called *squarefree* if it is not divisible by a square greater than 1. Prove that the exponent of B/A (as defined in Exercise 94) is squarefree.

Exercise 102. By an *extraspecial pair* we mean a pair consisting of a group B and a field l such that $\big(B : Z(B)\big)$ is finite, $[B, B]$ is a subgroup of $Z(B)$, and $Z(B)$ is a subgroup of l^*. The l-algebra $l\{B\}$ associated to such a pair is the group ring $l[B]$ modulo the ideal generated by the elements $\{a \cdot 1 - 1 \cdot a : a \in Z(B)\}$.
(a) Show that the quaternion group Q of order 8 forms an extraspecial pair with the field $\mathbf{R}$ of real numbers. To which well-known $\mathbf{R}$-algebra is $\mathbf{R}\{Q\}$ isomorphic?
(b) Let (B, l) be an extraspecial pair. Exhibit a ring homomorphism $l[Z(B)] \to l$ such that there is an l-algebra isomorphism $l\{B\} \cong l[B] \otimes_{l[Z(B)]} l$.
(c) Prove that there is a positive integer m not divisible by $\mathrm{char}\ l$ such that $\dim_l l\{B\} = \big(B : Z(B)\big) = m^2$.

Exercise 103. (This is an exercise for students who are willing to check the literature for a few auxiliary results.) Let (B, l) be an extraspecial pair with $\big(B : Z(B)\big) = m^2$, as in Exercise 102.
(a) Prove that every short exact sequence of $l\{B\}$-modules splits. (*Note.* A ring with this property is called *semisimple*.) (*Hint.* Check Maschke's theorem in the literature, and adapt its proof.)
(b) Prove $l = Z\big(l\{B\}\big)$, and that there exist a division ring D with $Z(D) = l$ and a positive integer n such that $l\{B\} \cong M(n, D)$ (as l-algebras) and $m^2 = n^2 \cdot \dim_l D$. (*Hint.* For the second part, use the classification of semisimple rings.)
(c) Suppose that l is finite. Prove: $l\{B\} \cong M(m, l)$ as l-algebras. (*Hint.* Apply Wedderburn's theorem on finite division rings.)