FREE GROUPS AND MONOIDS

Abstract. Free groups. Free commutative monoids, partitions and Segre characteristics.

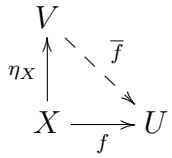
1. Free groups

Let X be a set. Let V be a (real) vector space with basis X. Consider the insertion $\eta_X \colon X \to V; x \mapsto x$ of the subset X into V. Then for each real vector space U, each function $f \colon X \to U$ has a unique linear extension $\overline{f} \colon U \to V$, defined by

$$(\lambda_1 x_1 + \cdots + \lambda_r x_r)\overline{f} = \lambda_1 x_1 f + \cdots + \lambda_r x_r f$$

for scalars $\lambda_1, \ldots, \lambda_r$ and elements $x_1, \ldots, x_r$ of X. The fact that $\overline{f}$ is an extension of f is expressed by the equation $\eta_X \overline{f} = f$. The fact that $\overline{f}$ is the unique linear extension of f is expressed conventionally by the commuting diagram

(1.1)



where the dashed format of the arrow labeled $\overline{f}$ records the existence and uniqueness of that function.

The vector space V with basis X may be described as the *free vector space* over the set X in the context of the diagram (1.1). In this context, it is best to think of V as the space

$$V = \left\{ \sum_{i=1}^{r} \lambda_i x_i \;\middle|\; r \in \mathbb{N},\ x_1, \ldots, x_r \in X,\ \lambda_1, \ldots, \lambda_r \in \mathbb{R} \right\} \tag{1.2}$$

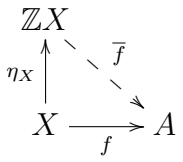
of all linear combinations of elements of the set X. Note that the vector 0 corresponds to the "empty" linear combination with $r = 0$ in (1.2).

1.1. **Free abelian groups.** Let X be a set. The *free abelian group* $\mathbb{Z}X$ over X is defined by a property analogous to the property expressed by the diagram (1.1). Specifically, define Λ or

$$\mathbb{Z}X = \left\{ \sum_{i=1}^{r} n_i x_i \;\middle|\; r \in \mathbb{N},\ x_1, \ldots, x_r \in X,\ n_1, \ldots, n_r \in \mathbb{Z} \right\} \tag{1.3}$$

as a subset of the vector space V in (1.2). Note that $(\mathbb{Z}X, +, 0)$ is an abelian subgroup of the abelian group $(V, +, 0)$. Also, note that the function $\eta_X \colon X \to V; x \mapsto x$ of (1.1) allows its codomain to be cut down to yield a new function $\eta_X \colon X \to \mathbb{Z}X; x \mapsto x$.

(1.4)



Proposition 1.1. *Let A be an abelian group. Then for each function $f \colon X \to A$, there is a unique group homomorphism*

$$\overline{f} \colon \mathbb{Z}X \to A; \sum_{i=1}^{r} n_i x_i \mapsto \sum_{i=1}^{r} n_i (x_i f)$$

such that $\eta_X \overline{f} = f$.

It is sometimes convenient to refer to the subset (1.3) of the free vector space V on X as a *lattice* Λ, a discrete set of position vectors carrying the free abelian group structure. (Compare Exercise 3.) One then reserves the notation $\mathbb{Z}X$ for the group structure itself, which may be considered as a group of translation vectors. The right regular representation of $\mathbb{Z}X$ given by Cayley's Theorem is then written as $(\Lambda, \mathbb{Z}X)$.

1.2. **Automata and free monoids.**

1.2.1. *Dynamical systems and automata.* A *dynamical system* (X, T) is a set X (called the *state space*) equipped with a function $T \colon X \to X$, the *evolution operator*. If an element x of the state space represents the state of a physical system at a given time, then xT is the state of the system one time unit later. The dynamical system is *reversible* if $T \colon X \to X$ is bijective.

More generally, an *automaton* (X, E) is a set X (again called the *state space*) equipped with a set E of functions $e \colon X \to X$, known as (*elementary*) *events*. If the system is in a state x, and event e occurs, then the system *transitions* to state xe. By convention of the model, the system is subject to no more than one event at any given time.

An automaton (X, E) may be described by a labeled graph (with loops), the *transition diagram*. For each event e, each state x is the tail of a directed edge $x \xrightarrow{e} xe$. If an event e does not change a state x, one may choose to omit the corresponding loop labeled e at x, thereby obtaining the transition diagram as a directed graph without loops.

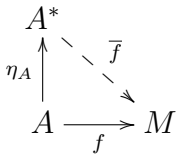
1.2.2. *Free monoids.* Let A be a set, described in the current context as an *alphabet*. For brevity, encode a tuple $(a_1, \ldots, a_n)$ from a direct power A^n as a string $a_1 \ldots a_n$, thus interpreting A^n as the set of *words of length* n in the alphabet A. In particular, write the singleton A^0 as $\{1\}$, so that 1 is the *empty word*.

Now define A^* to be the disjoint union $\sum_{n\in\mathbb{N}} A^n$. A monoid $(A^*, \cdot, 1)$ is defined on A^* by the *concatenations*

$$A^m \times A^n \to A^{m+n}; (a_1 \ldots a_m, b_1 \ldots b_n) \mapsto a_1 \ldots a_m b_1 \ldots b_n$$

for positive integers m, n. On the strength of the proposition below, the monoid A^* becomes the *free monoid* on the set A, with the function $\eta_A \colon A \to A^*; a \mapsto a$ inserting letters as words of length 1.

(1.5)



Proposition 1.2. *Let M be a monoid. For each function $f \colon A \to M$, there is a unique monoid homomorphism*

$$\overline{f} \colon A^* \to M; a_1 a_2 \ldots a_r \mapsto (a_1 f)(a_2 f) \ldots (a_r f)$$

such that $\eta_A \overline{f} = f$.

Corollary 1.3. *Let (X, E) be an automaton. Then for the insertion $j \colon E \hookrightarrow X^X; e \mapsto e$, the extension $\overline{j} \colon E^* \to X^X$ yields a representation of E^* on X.*

Remark 1.4. In the context of Corollary 1.3, words from E^* may be described as *compound events* of the automaton (X, E), to distinguish from the elementary events in the alphabet E.

1.2.3. *Free semigroups.* Given a set A, the set A^+ of words of positive length with letters from the alphabet A forms a subsemigroup of A^*. This semigroup is known as the *free semigroup* on the set A, since analogues of (1.5) and Proposition 1.2 may be formulated (Exercise 4).

Definition 1.5. A subset C of A^+ is a *code* over the alphabet A if

$$\forall\ 0 < m, n \in \mathbb{Z}\,,\ \forall\ c_1, \ldots, c_m, d_1, \ldots, d_n \in C\,,$$
$$c_1 \ldots c_m = d_1 \ldots d_n \ \Rightarrow\ m = n\,,\ c_1 = d_1\,,\ \ldots, c_m = d_m\,.$$

1.3. **Action on trees.** Let X be a set. The goal is to construct a group XG, together with a function $\eta_X\colon X \to XG$, such that for each function $f\colon X \to M$ from X to a group M, there is a unique group homomorphism $\overline{f}\colon XG \to M$ such that $\eta_X\overline{f} = f$:

(1.6)
$$\begin{array}{ccc} XG & & \\ {\scriptstyle\eta_X}\uparrow & \searrow^{\overline{f}} & \\ X & \xrightarrow[f]{} & M \end{array}$$

The group XG is known as the *free group* over the set X.

The free abelian group $\mathbb{Z}X$ over X, constructed in §1.1, emerged with a representation $(\Lambda, \mathbb{Z}X)$ by translation vectors acting on the lattice Λ of point vectors. The construction of the free group is similar, but more complex. The free group will be described by the action of an automaton, whose state space will be (the vertex set of) a tree Γ. Figure 1 illustrates the tree for the free group over the two-element set $\{x_1, x_2\}$.

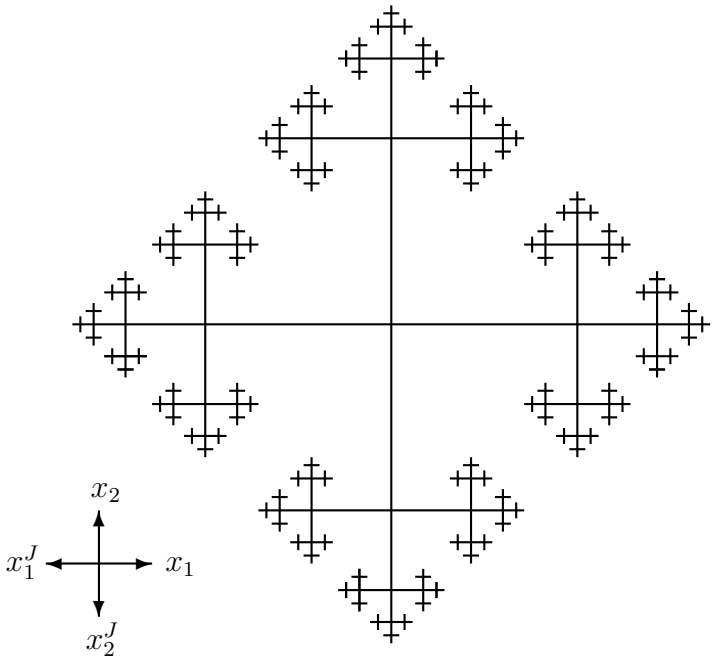


FIGURE 1. Tree structure for the free group on two generators.

Given the set X, let $A = X + XJ$ be the disjoint union of two copies of the set X. The insertions are $x \mapsto x$ and $x \mapsto x^J$. Define the map

$J\colon A \to A$ with $J^2 = 1_A$ by $J\colon x \mapsto x^J$. Let Γ denote the subset of the free monoid A^* consisting of those words in the alphabet A in which no letter a is immediately followed by a^J. For $x_1, x_2 \in X$, the word $x_1 x_2^J x_1 x_2$ lies in Γ, but the word $x_1 x_2^J x_2 x_1$ does not.

The automaton (Γ, A) will now be constructed. Consider an element a^J of A. The state space Γ decomposes into two parts: the set Γ_a of words ending in a, and its complement $\overline{\Gamma}_a$. The elementary event a^J then acts as follows:

$$a^J\colon \begin{cases} pa \mapsto p & \text{for } pa \in \Gamma_a\,; \\ q \mapsto qa^J & \text{for } q \in \overline{\Gamma}_a\,. \end{cases}$$

This elementary action is invertible, and its two-sided inverse is the action of a.

Since the composition of bijections is bijective, compound actions of the automaton (Γ, A) also biject. The inverse of the compound action of a word $a_1 \dots a_n$ in A^* is the compound action of the word $a_n^J \dots a_1^J$. Thus the image of A^* under the representation $r\colon A^* \to \Gamma^\Gamma$ given by Corollary 1.3 is actually a subgroup of Γ!. This subgroup is defined to be the free group XG. Thus the representation yields a monoid homomorphism

$$r\colon A^* \to XG\,.$$

Furthermore, there is the insertion $\eta_X\colon X \to XG; x \mapsto x^r$.

1.4. **The free group XG on the set X.**

1.4.1. *Group equivalence.* Let $u = a_1 \dots a_m$ and v be words in A^*, with letters $a_1, \dots, a_m$. The word v is said to be (obtained from u by) an *elementary reduction* of u if $a_i a_{i+1} = aa^J$ for some $1 \le i < m$ and a in A, and then $v = a_1 \dots a_{i-1} a_{i+2} \dots a_m$. Successive application of at most $\lfloor m/2 \rfloor$ elementary reductions to u reduces it to a word in Γ that is the result $1u^r$ of acting on 1 in Γ by the compound event u of A^*. Two words u, v in A are said to be *group equivalent* if and only if $1u^r = 1v^r$. Note that group equivalence is an equivalence relation, the relation kernel of the function $A^* \to \Gamma; u \mapsto 1u^r$. Moreover, Γ is a full set of representatives for the equivalence classes. The element $1u^r$ of Γ is called the (*completely*) *reduced form* or *normal form* of u.

1.4.2. *Extension to a homomorphism.* Let $f\colon X \to M$ be a function from the set X to a group M. The extension $\overline{f}$ of (1.6) will be constructed. Initially, the function extends to $f\colon A \to M$ by $x^J f = (xf)^{-1}$ for $x \in X$. By the free monoid property (1.5), there is a unique monoid

homomorphism $f'\colon A^* \to M$ extending $f\colon A \to M$. If $u = saa^J t$ and $v = st$ in A^*, then

$$\begin{aligned} uf' &= saa^J tf' \\ &= sf' \cdot af \cdot a^J f \cdot tf' \\ &= sf' \cdot af \cdot (af)^{-1} \cdot tf' \\ &= sf' \cdot tf' = stf' = vf' \,, \end{aligned}$$

so that group-equivalent words u, v in A^* have the same images uf', vf' in the group M.

Lemma 1.6. *The set Γ of A^* carries a well-defined group structure*

$$p \cdot q = pq^r \tag{1.7}$$

that makes it isomorphic to the group XG.

Proof. In the considerations above, interpret the function $f\colon X \to M$ as $\eta_X\colon X \to XG; x \mapsto x^r$. Then for u, v in Γ, the group-equivalence $1u^r = 1v^r$ implies $u\eta'_X = v\eta'_X$, so that $pu^r = pv^r$ for all p in Γ. In other words, the map

$$\theta\colon XG \to \Gamma; u^r \mapsto 1u^r \tag{1.8}$$

is injective. Since $p = 1p^r$ for p in Γ, the map θ of (1.8) is also surjective. With the product in Γ defined by (1.7), the map θ becomes a group isomorphism. Indeed, one has

$$(p^r q^r)\,\theta = (pq)^r\theta = 1(pq)^r = 1p^r q^r = pq^r = p \cdot q = 1p^r \cdot 1q^r = p^r\theta \cdot q^r\theta$$

for general elements p^r and q^r of XG, with p and q in Γ. □

Now consider the monoid homomorphism $f'\colon A^* \to M$. Then for p and q in Γ, one has $pf' \cdot qf' = pqf' = pq^r f' = (p \cdot q)f'$. Thus the monoid homomorphism $f'\colon A^* \to M$ restricts to a group homomorphism $f'\colon (\Gamma, \cdot, 1) \to M$. Finally, define

$$\overline{f} = \theta f'\colon XG \to \Gamma \to M \tag{1.9}$$

as the composite group homomorphism. Since

$$x\eta_X\overline{f} = x^r\theta f' = 1x^r f' = xf' = xf$$

for x in X, the homomorphism (1.9) gives the required extension of $f\colon X \to M$.

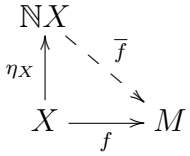
2. Free commutative semigroups and partitions

2.1. **Free commutative monoids.** Let X be a set. There are many ways to build a free commutative monoid $\mathbb{N}X$ on X. Mimicking §1.1, one may take

$$\mathbb{N}X = \left\{ \sum_{i=1}^{r} n_i x_i \;\middle|\; r \in \mathbb{N},\ x_1, \ldots, x_r \in X,\ n_1, \ldots, n_r \in \mathbb{N} \right\} \tag{2.1}$$

as a subset of the vector space V in (1.2). Note that $(\mathbb{N}X, +, 0)$ is a submonoid of the commutative monoid $(V, +, 0)$. Also, note that the function $\eta_X \colon X \to V; x \mapsto x$ of (1.1) allows its codomain to be cut down to yield a new function $\eta_X \colon X \to \mathbb{N}X; x \mapsto x$.

(2.2)



Proposition 2.1. *Let M be a commutative monoid. Then for each function $f \colon X \to M$, there is a unique monoid homomorphism*

$$\overline{f} \colon \mathbb{N}X \to M; \sum_{i=1}^{r} n_i x_i \mapsto \prod_{i=1}^{r} (x_i f)^{n_i}$$

such that $\eta_X \overline{f} = f$.

2.1.1. *Other interpretations.* A natural-number linear combination

$$n_1 x_1 + \cdots + n_r x_r$$

appearing in (2.1) may be interpreted as a *multiset*

$$\left\langle \overbrace{x_1, \ldots, x_1}^{n_1 \text{ times}}, \ldots, \overbrace{x_r, \ldots, x_r}^{n_r \text{ times}} \right\rangle \tag{2.3}$$

where the particular order in which elements appear is irrelevant (just as in ordinary sets), but where the multiplicity of occurrence of each element *is* counted. The empty linear combination 0 corresponds to the empty multiset $\langle\ \rangle$. The free monoid operation, addition of linear combinations, is taken as a union for multisets. Thus

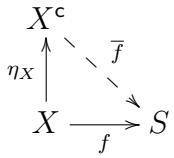
$$\langle 1, 1, 1, 2 \rangle \cup \langle 1, 3 \rangle = \langle 1, 1, 1, 1, 2, 3 \rangle ,$$

for example. Sometimes, the multiset (2.3) is written with a *power notation* as $x_1^{n_1} \ldots x_r^{n_r}$. In this convention, the monoid operation (just juxtaposition) is taken multiplicatively, and zero-th powers give the identity element of the monoid.

By (2.2), the constant function $f\colon X \to \mathbb{N}; x \mapsto 1$ extends to a monoid homomorphism $\overline{f}\colon \mathbb{N}X \to \mathbb{N}$. The value $|S|$ of $\overline{f}$ at a multiset S is known as the *size* of the multiset. For example, $|\langle 1,1,1,2\rangle| = 4$.

2.2. **Free commutative semigroups.** Let X be a set. The set of non-zero elements of the free commutative monoid $(\mathbb{N}X, +, 0)$ forms the *free commutative semigroup* X^{c} on X. As usual, there are appropriate analogues of (2.2) and Proposition 2.1:

(2.4)



Proposition 2.2. *Let S be a commutative semigroup. Then for each function $f\colon X \to S$, there is a unique semigroup homomorphism*

$$\overline{f}\colon X^{\mathsf{c}} \to S; \sum_{i=1}^{r} n_i x_i \mapsto \prod_{i=1}^{r} (x_i f)^{n_i}$$

such that $\eta_X \overline{f} = f$.

Remark 2.3. The other interpretations of free commutative monoid elements discussed in §2.1.1 apply in particular to the non-identity elements, as free commutative semigroup elements.

2.3. **Integer partitions.** Denote the singleton semigroup $(\{1\}, \cdot)$ by 1. As in §2.2, the free commutative semigroup 1^{c} may be identified with the semigroup $(\mathbb{Z}^+, +)$ of positive integers under addition. Thus the free commutative semigroup over $\mathbb{Z}^+$ is 1^{cc}. Elements λ of 1^{cc} are called *integer partitions*.

In accord with Remark 2.3, various notations for integer partitions are used, such as the *sum form*, e.g., $4+2+2+1$, or the *product form*, e.g., $4^1 2^2 1^1$ or $4^1 3^0 2^2 1^1$, or the *multiset form* $\langle 4,2,2,1\rangle$. The elements of the multiset are called the *parts* of the partition.

The constant function $1^{\mathsf{c}} \to 1^{\mathsf{c}}$ with image 1 extends to a semigroup homomorphism $1^{\mathsf{cc}} \to 1^{\mathsf{c}}$ whose values $|\lambda|$ give the *length* of a partition λ, the size of the multiset or the number of parts. For example, the length of the partition $4+2+2+1$ is 4.

The identity function $\mathrm{id}_{1^{\mathsf{c}}}\colon 1^{\mathsf{c}} \to 1^{\mathsf{c}}$ also extends to a semigroup homomorphism $\overline{\mathrm{id}_{1^{\mathsf{c}}}}\colon 1^{\mathsf{cc}} \to 1^{\mathsf{c}}$, whose values give the *sum* of a partition. For example, the sum of the partition $4+2+2+1$ is 9. For a partition λ, the functional relationship $\lambda\,\overline{\mathrm{id}_{1^{\mathsf{c}}}} = n$ is written conventionally as $\lambda \vdash n$.

2.3.1. *Segre characteristics.* Elements of 1^{ccc} are multisets of multisets of positive integers. They are known as *Segre characteristics*. Note that a classically written Segre characteristic such as [(22)3(11)] denotes the multiset $\langle\langle 2,2\rangle,\langle 3\rangle,\langle 1,1\rangle\rangle$ of multisets.

Segre characteristics are used to specify the blocks in the Jordan normal form of a matrix over an algebraically closed field, such as the field of complex numbers. For example, the Jordan normal form

$$\left[\begin{array}{cccccccccc}
\lambda_1 & 1 & & & & & & & & \\
 & \lambda_1 & & & & & & & & \\
\hline
 & & \lambda_1 & 1 & & & & & & \\
 & & & \lambda_1 & & & & & & \\
\hline
 & & & & \lambda_2 & 1 & & & & \\
 & & & & & \lambda_2 & 1 & & & \\
 & & & & & & \lambda_2 & & & \\
\hline
 & & & & & & & & \lambda_3 & \\
\hline
 & & & & & & & & & \lambda_3
\end{array}\right]$$

corresponds to the Segre characteristic [(22)3(11)].

2.4. **Conjugacy classes of symmetric groups.** One of the primary algebraic applications of integer partitions is the specification of the conjugacy classes in a symmetric group S_n for a positive integer n.

Let p be a permutation of $\underline{n}$, i.e., an element of S_n. The set of powers

$$p^{\mathbb{Z}} = \{p^r \mid r \in \mathbb{Z}\}$$

forms a subgroup of S_n. The $p^{\mathbb{Z}}$-set $\underline{n}$ decomposes as a disjoint union of orbits. If the respective orbit sizes are $n_1 \geq n_2 \geq \ldots \geq n_l$, then $n_1 + n_2 + \ldots + n_l$ is the sum form of a partition of n, the *cycle type* of p.

Theorem 2.4. *Suppose $\lambda \vdash n$. Then the set of all permutations of $\underline{n}$ with cycle type λ forms a conjugacy class C_λ of S_n. Indeed,*

$$S_n = \sum_{\mu \vdash n} C_\mu$$

is the orbit decomposition of S_n under the conjugacy action.

Remark 2.5. The proof of Theorem 2.4 is assigned as Exercise 18. Recall that on a $p^{\mathbb{Z}}$-orbit $\{x_i \mid i \in \mathbb{Z}/_k\}$ of length k, a permutation p acts as a cycle $(x_0\ x_1\ \ldots\ x_{k-1})$: $x_i \mapsto x_{i+1}$ of length k. Two cycles $(x_0\ x_1\ \ldots\ x_{k-1})$ and $(y_0\ y_1\ \ldots\ y_{k-1})$ of length k are conjugate by a permutation with $x_i \mapsto y_i$ for $i \in \mathbb{Z}/_k$. A permutation of cycle type $n_1 + n_2 + \ldots + n_l$ may be constructed as the product of disjoint cycles of respective lengths $n_1, n_2, \ldots, n_l$.

3. Exercises

(1) Verify Proposition 1.1.
(2) Suppose that there is a set bijection $b\colon X \to Y$. Show that the free abelian groups $\mathbb{Z}X$ and $\mathbb{Z}Y$ are isomorphic.
(3) For the respective choices

Square lattice:

$$\{(1,0),(0,1)\}$$

Rectangular lattice:

$$\{(1,0),(0,2)\}$$

Rhombic lattice:

$$\{(0,2),(1,1)\}$$

Oblique lattice:

$$\{(0,3),(1,1)\}$$

Triangular lattice:

$$\left\{(0,1)\,,\left(-\frac{1}{2},\frac{\sqrt{3}}{2}\right)\right\}$$

of the set X, draw the lattice Λ underlying the free abelian group $\mathbb{Z}X$ in the plane. Compare with this online list of lattices.
(4) Formulate and prove the freeness claims of §1.2.3.
(5) Show that $\{0, 01, 10\}$ is not a code over $\{0, 1\}$.
(6) Given an alphabet A of size at least 3, fix one particular element, and call it the *comma*. A *comma code* C is a subset of A^* consisting of words, in each of which the comma appears just once, namely at the end. Show that C is a code over A.
(7) A word v in A^* is said to appear as a *proper suffix* in a word w if there is a word u in A^+ such that $w = uv$. A subset C of A^* is a *suffix code* if no element of C appears as a proper suffix of another. Show that a suffix code is a code over A.
(8) Consider the context of §1.4.1. Suppose that a word u of length m is group equivalent to 1. Show that m is even.
(9) For a singleton set X, show that $\mathbb{Z}X$ and XG are isomorphic.
(10) Show that a bijection $b\colon X \to Y$ extends to an isomorphism $\overline{b}\colon XG \to YG$.
(11) Let $X = \{x_1, x_2\}$. Consider a function $f\colon X \to S_3$ in which $x_1 f$ has order 2 and $x_2 f$ has order 3. Determine the respective function values under the extension $\overline{f}\colon XG \to S_3$ for reduced words of length less than 4 in the alphabet $\{x_1, x_2, x_1^{-1}, x_2^{-1}\}$.

(12) Let M be a group. Let $\{H_i \mid i \in I\}$ be a set of subgroups of M. Show that the intersection

$$\bigcap\{H_i \mid i \in I\} = \{x \in M \mid \exists\, i \in I\,.\, x \in H_i\}$$

is a subgroup of M.

(13) Let X be a subset of a group M. Let $j\colon X \hookrightarrow M$ be the inclusion of X in M. Consider the homomorphic extension $\overline{j}\colon XG \to M$. The image of $\overline{j}$ is called the *subgroup* $\langle X\rangle$ of M *generated* by X.
   (a) Show directly that $\langle X\rangle$ is a subgroup of M.
   (b) Show that $\langle X\rangle$ is the intersection of the set of subgroups of M that contain X.

(14) Show that the inclusion $P \hookrightarrow \mathbb{Z}^+$ of the set P of prime numbers in the set of positive integers extends to a monoid isomorphism $\mathbb{N}P \to (\mathbb{Z}^+, \cdot, 1)$. This is the classical Fundamental Theorem of Arithmetic.

(15) List all 7 partitions that sum to 5.

(16) Derive Euler's formula

$$1 + \sum_{n=1}^{\infty} p(n)x^n = \prod_{m=1}^{\infty}(1 - x^m)^{-1}$$

for the number $p(n)$ of partitions of a positive integer n.

(17) List all the possible Segre characteristics for the Jordan normal forms of 4×4-matrices over $\mathbb{C}$.

(18) Prove Theorem 2.4.

(19) For the partition $\lambda = n_1 + \ldots + n_l$ of a positive integer n, determine the size of the conjugacy class C_λ in S_n.

(20) In the group S_4, determine which unions of conjugacy classes form subgroups of S_4.