MA 572
COMBINATORICS II
Permutation groups, designs and enumeration

Jürgen Bierbrauer

May 8, 1997

Contents

Chapter 1

Introduction to Group Theory

Definition (1.1) *Let G be a set and let a product operation* $: G \times G \longrightarrow G$ *be defined. Then $(G, \cdot)$ is a* **group** *if the following hold:*

- $g_1(g_2g_3) = (g_1g_2)g_3$ *for all $g_i \in G$ (***associativity***).*
- *There is an element $1 \in G$ (the* **neutral element***) such that $1g = g1 = g$ for all $g \in G$.*
- *For every $g \in G$ there is an element $g^{-1} \in G$ (the* **inverse element***) such that $gg^{-1} = g^{-1}g = 1$.*

Observe that the neutral element is uniquely determined (if $1'$ is a neutral element, then by definition $11' = 1 = 1'$). The following **cancellation laws** hold in any group: if $ax = ay$, then $x = y$ and analogously: if $xa = ya$, then $x = y$. It follows that the inverse is uniquely determined and that equations $ax = b$ and $xa = b$ have unique solutions x ($x = a^{-1}b$ in the first case, $x = ba^{-1}$ in the second case).
A group G is **finite** if the set G is finite. The cardinality of G is then called the **order** of the group. A group G is **commutative** (or **abelian**) if $ab = ba$ for all $a, b \in G$.

Example (1.1)

- *The integers $\mathbb{Z}$ form an abelian group with addition as group operation. The neutral element is 0, the inverse of a is $-a$.*
- *If V is a vector space, then $(V, +)$ is by definition an abelian group.*

- *If K is a field, then $(K - \{0\}, \cdot)$ is an abelian group, the multiplicative group of K.*
- *The* **cyclic group** Z_n *: imagine n objects, without restriction $\{0, 1, 2, \ldots, n-1\}$ arranged in a circle. The group Z_n consists of clockwise rotations and has order n.*

Example (1.2) (symmetric group) *The* **symmetric group** S_n *consists of all permutations of a set of n objects. The group operation is composition of functions. The neutral element is the permutation, which fixes every object. The order of S_n clearly is $|S_n| = n!$ For $n \geq 3$ the group S_n is non-abelian.*

Example (1.3) (general linear group) *Let $V = V(n, K)$ be an n-dimensional vector space over the field K. The group $GL(n, K)$ is defined as the set of all invertible linear mappings : $V \longrightarrow V$. The group operation is composition of functions. A linear mapping $\alpha : V \longrightarrow V$ is in $GL(n, K)$ if and only if $det(\alpha) \neq 0$. Because of the multiplicativity of the determinant ($det(\alpha\beta) = det(\alpha) \cdot det(\beta)$) and because a field does not have divisors of zero we see that $GL(n, K)$ is indeed a group.*
Let $K = \mathbb{F}_q$ be a finite field (recall that q is a prime-power). We write then $GL(n, q)$. The order of $GL(n, q)$ is the number of ordered bases of V. We obtain

$$|GL(n, q)| = (q^n - 1)(q^n - q) \cdot \ldots (q^n - q^{n-1}) = q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1).$$

Some basic notions are very natural:

Definition (1.2) (subgroups) *A subset $H \subseteq G$ of the group G is a* **subgroup** *if for every $h \in H$ we have $h^{-1} \in H$ and for every $h_1, h_2 \in H$ we have $h_1 h_2 \in H$. In words: H is a subgroup if it is closed under inverses and products. In particular H is then a group in its own right. We write then $H \leq G$ or $H < G$.*

Definition (1.3) (homomorphisms) *Let G_1, G_2 be groups. A mapping $\alpha : G_1 \longrightarrow G_2$ is a* **(group) homomorphism** *if the following always hold:*

$$(g_1 g_2)\alpha = (g_1\alpha)(g_2\alpha).$$

$$g^{-1}\alpha = (g\alpha)^{-1}.$$

(This means that α respects the group structures). Let α be a homomorphism. α is an **isomorphism** *if it is bijective. In that case we say that G_1 and G_2 are* **isomorphic:** $G_1 \cong G_2$.

Isomorphic groups have the same group structure. It follows that for most purposes we will have to consider isomorphism classes of groups only. The next question to consider is the following: let the group order $|G|$ be given. What can be said about the orders of subgroups in general?

Definition (1.4) (cosets) *Let $H \subseteq G, g \in G$. The set $Hg = \{hg|h \in H\}$ is a* **right coset** *of H in G. The left coset gH is analogously defined.*

If H is finite, then $|gH| = |Hg| = |H|$ for every $g \in G$, as follows from the cancellation laws.

Lemma (1.1) *Let G be a finite group, $H < G$. Then the following hold:*

- *If $g' \in Hg$, then $Hg' = Hg$.*
- *If $Hg' \neq Hg$, then $Hg' \cap Hg = \emptyset$.*

Proof: If $g' \in Hg$, then $g' = h_0 g$ for some $h_0 \in H$. For every $h \in H$ we have $hg' = hh_0 g \in Hg$, and also $hg = hh_0^{-1}h_0 g = hh_0^{-1}g' \in Hg'$. We obtain $Hg = Hg'$. The second statement is now obvious.■

This leads us to the first interesting theorem of group theory:

Theorem (1.1) (Lagrange's theorem) *If H is a subgroup of the finite group G, then the order of H divides the order of G.*

Proof: Denote by G/H the collection of right cosets of H in G. We have seen that the right cosets partition G and the number of elements in each such coset equals the order of H. This proves our Theorem.■

Definition (1.5) (index) *Let $H \leq G$. The* **index** $[G : H]$ *of H in G is the number of cosets of H in G,*

$$[G : H] = |G/H| = |G|/|H|.$$

It is now natural to ask for which divisors of $|G|$ there exists a subgroup $H < G$ of that order. An important partial answer will be given by Sylow's theorems. The next question we have to study is the definition of factor groups. So let a subgroup $H < G$ be given. Is it possible to give the set G/H the structure of a group, which is inherited from the group structure of G? We know that this is possible for example in the case of vector spaces. Let us study this problem in general: We have to define the group structure on the set G/H of right cosets as follows: $(Ha)(Hb) = Hab$. The question is if this definition makes sense. Replace a and b by other representatives from the same cosets: ha and $h'b$ respectively. We must prove that the product coset is the same, hence that $(ha)(h'b) = h''ab$ for some $h'' \in H$. As $(ha)(h'b) = h(ah'a^{-1})ab$ this is equivalent with $ah'a^{-1} \in H$. This condition has to be satisfied for all $h' \in H$ and all $a \in G$. We conclude that a factor group G/H can be defined if and only the following condition is satisfied for all $g \in G : g^{-1}Hg = H$, or equivalently $Hg = gH$. This leads us to the definition of a normal subgroup:

Definition (1.6) (normal subgroup) *A subgroup $N \leq G$ is a* **normal subgroup** *if and only if $Ng = gN$, equivalently $g^{-1}Ng = N$ for all $g \in G$. In that case we write $N \lhd G$, respectively $N \unlhd G$.*

Definition (1.7) (factor group) *Let $N \unlhd G$. The* **factor group** *G/N is the set of all (right or left) cosets of N in G, where the product is defined by*

$$(Ng)(Ng') = Ngg'.$$

We have seen above that this definition makes sense as N is a **normal** subgroup.

Problem (1.1)

- *Determine the neutral element of the factor group G/N.*
- *Determine the order of the factor group G/N.*

If $N \lhd G$, then G can be thought of as built from N and from G/N. In that perspective group theory falls into two parts:

- study of groups G that do not possess nontrivial normal subgroups, and

- study the structure of G when N and G/N are given.

Definition (1.8) (simple groups) *A group G which does not possess non-trivial normal subgroups is called a* **simple group.** *Here trivial normal subgroups are G itself and $\{1\}$.*

Lemma (1.2) *Let $\alpha : G_1 \longrightarrow G_2$ be a group homomorphism. Then the following hold:*

1. *The image $Im(\alpha)$ of α is a subgroup of G_2.*
2. *Put $ker(\alpha) = \{g | g \in G_1, g\alpha = 1\}$ (the* **kernel** *of α). Then $ker(\alpha) \trianglelefteq G_1$.*
3. *α is injective if and only if $ker(\alpha) = \{1\}$.*
4. *$Im(\alpha) \cong G_1/ker(\alpha)$ (the* **first isomorphism theorem***).*

Proof: The first statement follows from $(g\alpha)(g'\alpha) = (gg')\alpha \in Im(\alpha)$ and $(g\alpha)^{-1} = (g^{-1})\alpha \in Im(\alpha)$. In the same fashion we see that $ker(\alpha) \leq G_1$. Is it a normal subgroup? Let $h \in ker(\alpha), g \in G_1$. Then $(g^{-1}hg)\alpha = (g\alpha)^{-1}(h\alpha)(g\alpha) = (g\alpha)^{-1}(g\alpha) = 1$, hence $g^{-1}hg \in ker(\alpha)$.
If α is injective, then clearly $ker(\alpha) = \{1\}$. Assume $ker(\alpha) = \{1\}$ and $g_1\alpha = g_2\alpha$. We have to show $g_1 = g_2$. In fact, as $(g_1^{-1}g_2)\alpha = 1$ we get $g_1^{-1}g_2 \in ker(\alpha)$, hence $g_1 = g_2$.
We define a mapping

$$\overline{\alpha} : G_1/ker(\alpha) \longrightarrow Im(\alpha)$$

by $ker(\alpha)g \mapsto g\alpha$. This mapping is well-defined as for every $h \in ker(\alpha)$ we have $(hg)\alpha = (h\alpha)(g\alpha) = g\alpha$. We claim that $\overline{\alpha}$ is an isomorphism. It is obvious that $\overline{\alpha}$ is a homomorphism and is surjective. Remains to prove the injectivity. So let a coset $ker(\alpha)g \in ker(\overline{\alpha})$. Equivalently $g \in ker(\alpha)$. This shows that $ker(\alpha)g = ker(\alpha)$, the neutral element of $G_1/ker(\alpha)$. ■

Problem (1.2) *Give an example showing that the image $Im(\alpha)$ of a homomorphism α is not in general a normal subgroup.*

Every normal subgroup $N \trianglelefteq G$ is the kernel of a homomorphism α. We can choose α as the **canonical homomorphism** $\alpha : G \longrightarrow G/N$ as defined by $g\alpha = Ng$. Observe also that every subgroup of an abelian group is a normal subgroup. Even in nonabelian groups it is important to study which elements commute.

Definition (1.9) (commutator) *Let $g_1, g_2 \in G$. The* **commutator** *of g_1, g_2 is defined as*

$$[g_1, g_2] = g_1^{-1} g_2^{-1} g_1 g_2.$$

Observe that $[g_1, g_2] = 1$ if and only if $g_1 g_2 = g_2 g_1$. In that case we say that g_1, g_2 commute.

Definition (1.10) (center) *Let $gz(G) = \{z | z \in G, [z, g] = 1 \text{ for all } g \in G\}$. So the center $\mathbb{Z}(G)$ is the set of all elements of G, which commute with every element of G.*

Problem (1.3) *Prove that the center $\mathbb{Z}(G)$ is a normal subgroup of G.*

Definition (1.11) (generators) *Let $S \subset G$. Denote by $< S >$ the smallest subgroup of G containing S. We call $< S >$ the subgroup of G* **generated** *by the set S. Clearly we have*

$$< S > = \{\prod_{i=0}^{n} s_i | n \in \mathbb{N}, s_i \in S \cup S^{-1}\} = \cap_{S \subseteq H \leq G} H.$$

This simplifies in the case when S has only one element:

Lemma (1.3) *Let $g \in G$ and $< g >$ the subgroup of G generated by the $\{g\}$. If all powers $g^n, n = 1, 2, \ldots$ are different, then $< g >$ is isomorphic to $(\mathbb{Z}, +)$. If not, let n be the smallest natural number such that $g^n = 1$. Then $< g > = \{1, g, g^2, \ldots, g^{n-1}\}$ is isomorphic with the cyclic group Z_n from Example (1.1). In that case n is called the* **order** *$o(g)$ of g. It is also the order of $< g >$.*

The proof is all but trivial. We leave it as an exercise. In the case when all the powers of g are different the isomorphism between $< g >$ and $\mathbb{Z}$ is given by $n \mapsto g^n$.

Lemma (1.4) *Let $A, B \leq G$. Then $A \cap B \leq G$.*

Again the proof is trivial.

Lemma (1.5) *If $A \leq G$ and $N \trianglelefteq G$, then $A \cap N \trianglelefteq A$.*

Proof: $[A, N \cap A] \subseteq N \cap A$.$\blacksquare$

Observe that the set $AB = \{ab | a \in A, b \in B\}$ is not in general a subgroup.

Lemma (1.6) *Let $A, B \leq G$ and assume that either A or B is a normal subgroup of G. Then $AB \leq G$.*

Proof: Assume without restriction A to be a normal subgroup. Then $aba'b' = a(ba'b^{-1})bb' \in AB$ as $ba'b^{-1} \in A$, and
$(ab)^{-1} = b^{-1}a^{-1} = (b^{-1}a^{-1}b)b^{-1} \in AB$ for the same reason. $\blacksquare$

In the general case, when neither A nor B are normal subgroups, we have no control on the size of the smallest subgroup $< A, B >$ containing A and B. A strengthening of this Lemma will be obtained as Problem (2.1).

Problem (1.4) *Let $H \leq G$. Prove that $H \trianglelefteq G$ if and only if $[H, G] \subseteq H$.*

Expressions like $[A, B]$ and S^{-1} are to be read in a settheoretic way, just as in the case of the product set AB. For example $[A, B] = \{[a, b] | a \in A, b \in B\}$.

Definition (1.12) (commutator subgroup) *The* **commutator group** G' *of G is the smallest subgroup containing all commutators, $G' =< [G, G] >$.*

Lemma (1.7) *We have $G' \trianglelefteq G$. A factor group G/N is abelian if and only if $N \geq G'$.*

Proof: In order to show that G' is a normal subgroup we have to show that $g^{-1}[x, y]g \in G'$ for all $x, y, g \in G$. It is an easy exercise to check that $g^{-1}[x, y]g = [xg, y][y, g]$, proving this claim.
A group G is abelian if and only if all commutators vanish (equal 1). This is equivalent with $G' = 1$. If this criterion is applied to G/N we see that G/N is abelian if and only if $[G, G] \subseteq N$, equivalently $G' \leq N$. $\blacksquare$

Corollary (1.1) *If G/N_1 and G/N_2 are abelian groups, then $G/(N_1 \cap N_2)$ is abelian, too.*

Proof: At first observe that $N_1 \cap N_2 \trianglelefteq G$. This is true as $[G, N_1 \cap N_2] \subseteq N_1 \cap N_2$. Furthermore, the fact that the factor groups for the N_i are abelian implies $[G, G] \subseteq N_1 \cap N_2$. The claim follows.∎

This is a first success of the use of commutators. The statement of the Corollary is not completely evident otherwise.

Definition (1.13) (automorphism group) *An* **automorphism** *of G is an isomorphism of G with itself. The automorphisms form a group, where the group operation (written as multiplication again) is composition of functions. $Aut(G)$ is the group of all automorphisms of G.*

Definition (1.14) (inner automorphisms) *Let $g \in G$. The mapping I_g, where $xI_g = g^{-1}xg$ is an automorphism of G (***conjugation** *with g). The mapping $I : G \longrightarrow Aut(G)$, which maps g to I_g, is a group homomorphism. Its image is called the group $Inn(G)$ of* **inner automorphisms** *of G. The kernel of I is $\mathbb{Z}(G)$. In particular $Inn(G) \cong G/\mathbb{Z}(G)$.*

Proof: I_g is a homomorphism: $xyI_g = g^{-1}xyg = (g^{-1}xg)(g^{-1}yg) = (xI_g)(yI_g)$, and $x^{-1}I_g = (xI_g)^{-1}$. Let $y \in G$ be given. The equation $g^{-1}xg = y$ possesses the unique solution $x = gyg^{-1}$. It follows that I_g is an automorphism.
I is a homomorphism: $xI_gI_{g'} = (g^{-1}xg)I_{g'} = g'^{-1}g^{-1}xgg' = xI_{gg'}$. Similarly $I_{g^{-1}} = I_g^{-1}$.
Assume $g \in ker(I)$. This means that I_g operates as the identity, hence $g^{-1}xg = x$ for all $x \in G$, equivalently $[g, x^{-1}] = 1$. Comparing with Definition (1.10) we see that this is equivalent with $g \in \mathbb{Z}(G)$. The isomorphism statement follows from the first isomorphism theorem as recorded in Lemma (1.2).

Theorem (1.2) (second isomorphism theorem) *If $N \trianglelefteq G$ and $A \leq G$, then*

$$NA/N \cong A/(N \cap A).$$

Proof: Let us make sure that everything makes sense. AN is a subgroup by Lemma (1.6), and N is of course normal in AN. By Lemma (1.5) $N \cap A \trianglelefteq A$. Let $\alpha : G \longrightarrow G/N$ be the canonical homomorphism β the restriction of α to A. Then $Im(\beta) = AN/N$. By the first isomorphism theorem (Lemma (1.2)) we have $AN/N \cong A/ker(\beta)$. As $ker(\beta) = (ker(\alpha) \cap A = N \cap A$ we are done.■

Definition (1.15) (centralizer, normalizer) *Let $A \subseteq G$. The* **centralizer** *of A in G is defined as*

$$\mathbb{C}_G(A) = \{g | g \in G, a^g = a \text{ for all } a \in A\}.$$

The **normalizer** *of A in G is defined as*

$$\mathbb{N}_G(A) = \{g | g \in G, A^g = A\}.$$

Observe that $A^g = A$ is equivalent with $[A, g] \subseteq A$.

Lemma (1.8) *Let $A \subseteq G$. Then $\mathbb{C}_G(A)$ and $\mathbb{N}_G(A)$ are subgroups of G and $\mathbb{C}_G(A) \trianglelefteq \mathbb{N}_G(A)$. Let $A \leq G$. Then the factor group $\mathbb{N}_G(A)/\mathbb{C}_G(A)$ is isomorphic to a subgroup of $Aut(A)$. We call $\mathbb{N}_G(A)/C\mathbb{C}_G(A)$ the group of automorphisms of A* **induced by** *G.*

Proof: It is clear that $\mathbb{C}(A) \leq \mathbb{N}(A)$ are subgroups. Let $h \in \mathbb{C}(A), g \in \mathbb{N}(A), a \in A$. Then $a^{h^g} = a^{g^{-1}hg} = a^{g^{-1}g} = a$ as $a^{g^{-1}} \in A$, and therefore is centralized by h. This shows $h^g \in \mathbb{C}(A)$. It follows $\mathbb{C}(A) \trianglelefteq \mathbb{N}(A)$.
Map $g \in \mathbb{N}(A)$ to the restriction of I_g to the subgroup A. This mapping is a homomorphism. Its image is contained in $Aut(A)$. An element $g \in A$ is in the kernel if and only $a^g = a$ for all $a \in A$, equivalently if $g \in \mathbb{C}(A)$. This proves our last claim.■

Problem (1.5) *Let $A \leq G$. Prove the following statements:*

1. *$A \leq \mathbb{N}_G(A)$.*
2. *$\mathbb{C}_G(A) \cap A = \mathbb{Z}(A)$.*
3. *$\mathbb{N}_G(A)$ is the largest subgroup H of G such that $A \trianglelefteq H$.*

Problem (1.6) *Prove the following strengthening of Lemma (1.6):*
If $A, B \leq G$ and $B \leq N(A)$, then $AB \leq G$.

Definition (1.16) (permutation representation) *A* **permutation representation** *π of G is a homomorphism $\pi : G \longrightarrow S_n$ (n is the* **degree** *of π). π is* **faithful** *if $ker(\pi) = 1$. The image of π is called a* **permutation group**.

Informally a permutation representation describes how G operates on a set of n objects as a group of permutations.

Definition (1.17) (orbits) *Let π be a permutation representation of G. Denote by Ω the n-element set on which G operates. The* **orbit** *of $x \in \Omega$ is*

$$x^G = \{y | y \in \Omega, xg = y \text{ for some } g \in G.$$

Here we have omitted π, identifying the operation of $g \in G$ with that of $g\pi$. A permutation representation π is **transitive** *if Ω is an (the) orbit.*

Definition (1.18) (stabilizer) *Let G be represented on the set Ω. For $g \in G$ put $F(g) = F_\Omega(g) = \{x | x \in \Omega, xg = x\}$ (the set of* **fixed points** *of g. For $x \in \Omega$ put $G_x = \{g | g \in G, gx = x\}$, the* **stabilizer** *of x.*

Lemma (1.9) (orbit length lemma) *Let G be represented on the set Ω and $x \in \Omega$. Then $G_x \leq G$ and the length of the orbit of x is given by*

$$|x^G| = [G : G_x].$$

Proof: It is clear that G_x is a subgroup. We define a mapping : $G \longrightarrow x^G$ by mapping g to x^g. This mapping is clearly surjective. As it is constant on every coset $G_x g$ we can consider it as a mapping : $G/G_x \longrightarrow x^G$. We claim that the mapping is also injective: if $xg = xh$, then $x(hg^{-1}) = x$, hence $hg^{-1} \in G_x$ and $G_x g = G_x h$. This shows that we have a bijection. The claim follows.■

Example (1.4) *Two permutation representations of G on the power set of G are particularly important:*

- **multiplication:** *g maps the subset K to Kg.*

- **conjugation:** *g maps the subset K to $K^g = g^{-1}Kg$.*

Let $K \leq G$. The orbit of K under the (right) multiplication representation is the set G/K of right cosets, the stabilizer of K is K. Let $K = \{k\}$ and consider the conjugation representation. The orbit of K is then $k^G = \{k^g | g \in G\}$, the stabilizer of k is the centralizer $\mathbb{C}_G(k)$.

Definition (1.19) (conjugacy class) *Let $g \in G$. The* **conjugacy class** *of g in G is*

$$g^G = \{h^{-1}gh | h \in G\}.$$

Observe that this is the orbit of g under the conjugation representation. A special case of Lemma (1.9) yields

$$|g^G| = [G : \mathbb{C}_G(g)].$$

Lemma (1.10) *Let $K \leq G$. The number of different conjugates K^g of the group K is $[G : \mathbb{N}_G(K)]$. Observe that conjugation is an automorphism, so that every conjugate of K is a subgroup of G, which is isomorphic to K.*

Proof: This is an application of Lemma (1.9) to the conjugation representation of G.

Definition (1.20) (p-groups) *Let p be a prime. A p-group is a finite group whose order is a power of p.*

Observe that by Lagrange's theorem subgroups and factor groups of p-groups are p-groups.

Theorem (1.3) (Sylow's theorems) *Let G be a finite group of order $p^n m$, where m is coprime to the prime p. Then the following hold:*

1. *G possesses a subgroup of order p^n (such subgroups are called p-* **Sylowsubgroups***).*

2. *All p-Sylowsubgroups of G are conjugate (in particular they are isomorphic). Their number is*

$$[G : \mathbb{N}_G(P)] \equiv 1 \ (mod\ p).$$

   Here P denotes a p-Sylowsubgroup.

3. *$P \leq G$ is a p-Sylowsubgroup of G if and only if P is a p-group and p does not divide $|I\!N_G(P)/P|$.*

4. *If $R \leq G$ is a p-group, then R is contained in a p-Sylowsubgroup.*

We will denote the set of all p-Sylowsubgroups of G by $Syl_p(G)$.

Proof (by Michael Josephy, Costa Rica): Let us denote by $Syl_p(G)$ the set of all p-subgroups of G, whichg are not contained in a larger p-subgroup.

Lemma (1.11) *Let the p-group P operate on the set Ω. Denote by $F_\Omega(P)$ the set of fixed points. Then $|F_\Omega(P)| \equiv |\Omega|$ (mod p).*

Proof: This is obvious as by Lemma (1.9) all orbits have lengths a power of p and the fixed points are precisely the orbits of length 1.■

Lemma (1.12) (Cauchy's theorem) *Let the order of G be divisible by p and $m \geq 1$. Then the number of solutions of equation $x^{p^m} = 1$ in G is a multiple of p. In particular G does contain elements of order p (equivalently subgroups of order p).*

Proof: Put $q = p^m, X = \{(x_1, x_2, \ldots, x_q)|x_i \in G, x_1x_2 \cdot \ldots x_q = 1\}$. We have $|X| = |G|^{q-1}$. If $x_1x_2 \cdot \ldots x_q = 1$ then also $x_2x_3 \cdot \ldots x_qx_1 = 1$. It follows that the cyclic permutation $(x_1, x_2, \ldots, x_q) \mapsto (x_2, \ldots, x_q, x_1)$ generates a p-group of permutations of X. The fixed points under this group are precisely the q-tupels $(a, a, \ldots, a)$, where $a^q = 1$. It follows that they are in bijection with the solutions of equation $x^q = 1$. As $|X|$ is a power of p we conclude from Lemma (1.11) that we are done.■

We continue with the proof of Theorem (1.3). Let $P \in Syl_p(G)$ and $X' = \{P^g|g \in G\}$. Clearly P operates on X' by conjugation. Let Q be a fixed point. This means that $Q \in Syl_p(G)$ such that Q is conjugate to P under the action of G and $P \leq I\!N(Q)$. It follows from Problem (2.1) that $PQ \leq P$. As $PQ/Q \cong P/(P \cap Q)$ by Theorem (1.2) we see that PQ is a p-group. The definition of $Syl_p(G)$ shows that $Q = P$. It follows that from Lemma (1.11) that the cardinality of X' is $\equiv 1$ (mod p).
We show next that $X' = Syl_p(G)$. Assume $R \in Syl_p(G) - X'$. We have seen

that $|X''| \equiv 1 \pmod p$. The operation of P shows, via the same argument, that $|X''| \equiv 0 \pmod p$, contradiction.
We have proved 2. Next we show that $|P| = p^n$.
Observe $[G : P] = [G : I\!N_G(P)][I\!N_G(P) : P]$. Assume $|P| < p^n$. Then $[G : P]$ is a multiple of p. We know that the first factor equals the cardinality of $Syl_p(G)$ and is not divisible by p. It follows $|I\!N_G(P)/P|$ is divisible by p. This contradicts the maximality of P as a p-subgroup of G. We conclude that $Syl_p(G)$ consists of the subgroups of order p^n. ■

Here is a first application of Sylow's theorems:

Theorem (1.4) (Frattini argument) *Let $P \le N \trianglelefteq G$, where $P \in Syl_p(G)$. Then $G = N I\!N_G(P)$.*

Proof: Let $g \in G$. Clearly $P^g \in Syl_p(N)$. As by Sylow's theorems all p-Sylowsubgroups of N are conjugate there must exist some $h \in N$ such that $P^g = P^h$. It follows $gh^{-1} \in I\!N(P)$, thus $g \in I\!N_G(P)N = N I\!N_G(P)$.■

Next we prove some basic properties of p-groups:

Theorem (1.5) (p-groups) *Let $P \neq 1$ be a p-group. Then the following hold:*

1. *If $1 \neq N \trianglelefteq P$, then $N \cap Z\!\!\!Z(P) \neq 1$. In particular $Z\!\!\!Z(P) \neq 1$.*
2. *If $Q < P$, then $I\!N_P(Q) > Q$. In particular $Q \triangleleft P$ if $[P : Q] = p$.*
3. *If P is nonabelian, then $[P : Z\!\!\!Z(P)] \ge p^2$ and $P/Z\!\!\!Z(P)$ is not cyclic.*

Proof: 1. Let P operate on the elements of N by conjugation. We know from Lemma (1.11) that the number of fixed points is divisible by p. These fixed points are precisely the elements of $Z\!\!\!Z(P) \cap N$.
2. Assume without restriction that Q is not a normal subgroup of P. The cardinality of the set X of all P-conjugates of Q is $[P : I\!N_P(Q)]$, a multiple of p. Let Q itself operate on X by conjugation. Lemma (1.11) shows that Q has more than one fixed point. Let $Q^g \neq Q$ be such a fixed point. Then $Q \le I\!N(Q^g)$, hence $Q^{g^{-1}} \le I\!N(Q)$.
3. Let $g \in P - Z\!\!\!Z(P)$. Then $< Z\!\!\!Z(P), g >$ is abelian ■

Next we want to construct new groups from old.

Definition (1.21) • *Let G, H be (isomorphism types of) groups. The Cartesian product $G \times H$ becomes a group by*

$$(g, h) \cdot (g', h') = (gg', hh').$$

This is the **(outer) direct product.** *Observe that multiplication in the first component is in G, multiplication in the second component happens in H.*

- *Let $A \leq Aut(G)$. Write the operation of $a \in A$ on G as a^g. The Cartesian product $G \times A$ becomes a group by*

$$(g, a) \cdot (g', a') = (g^{a'} g', aa').$$

This is the **semidirect product** *$G \cdot A$. Identify $g \in G$ with $(g, 1)$ and $a \in A$ with $(1, a)$. Then the group operations in the product group when restricted to G or to A are group operations in these groups. Moreover $a^{-1}ga = (1, a^{-1})(g, 1)(1, a) = (g, a^{-1})(1, a) = (g^a, 1) = g^a$. We see that we have represented the application of automorphism a to element g as conjugation in the semidirect product. Observe also that $G \trianglelefteq G \cdot A$.*

Definition (1.22) (elementary abelian groups) *Let p be a prime. The* **elementary abelian group** *$E(p^n)$ of order p^n is the direct product of n copies of Z_p. Observe that $E(p^n)$ is isomorphic with the additive group of the vector space $V(n, p)$. Every nonidentity element of $E(p^n)$ has order p. As an automorphism of $E(p^n)$ is by definition the same as an invertible linear mapping of $V(n, p)$ onto itself we have*

$$Aut(E(p^n)) \cong GL(n, p) \text{ (compare Example (1.3))}.$$

In particular $Aut(Z_p) \cong Z_{p-1}$.

Lemma (1.13) (calculation in cyclic groups) *Let $< x > \cong Z_n$.*

1. *If $gcd(n, m) = 1$, then $< x^m > = < x >$.*
2. *In general $o(x^m) = n/gcd(n, m)$.*
3. *If n and m are coprime, then $Z_n \times Z_m \cong Z_{nm}$.*

4. *Let* $n = \prod_i p_i^{a_i}$*, where the* p_i *are different primes. Put*
$$\phi(n) = \prod_i (p_i^{a_i} - p_i^{a_i - 1}) = n \prod_{p|n} (1 - 1/p)$$
(the **Euler phi-function***). Then* $\phi(n) = |\{m | 0 < m < n, gcd(m,n) = 1\}| = |Aut(Z_n)|$ *and* $\phi(n)$ *is the number of generators of* Z_n*.*

5. *If* $m|n$*, then* $< x^{n/m} >$ *is the unique subgroup of order* m *of* Z_n*.*

Proof: Let $gcd(m,n) = 1$. By the Euclidean algorithm we can write $1 = ma + nb$ with integers a, b. It follows $x = x^{ma+nb} = (x^m)^a$. This shows that x^m is a generator of Z_n.
2. $x^{ma} = 1$ is equivalent with $n|ma$. The minimum a achieving this is $a = n/gcd(n,m)$.
3. Let x be a generator of Z_n and y a generator of Z_m. We claim that xy generates the direct product. This is the case as $< (xy)^n > = < x^n y^n > = < y^n > = < y >$ and analogously $< (xy)^m > = < x >$.
4. This is an easy exercise.
5. We have that $o(x^{n/m}) = m$. Let $x^{im} = 1$. This is equivalent with i being a multiple of n/m. There are m such group elements. It follows that the subgroup of order m of Z_n consists of all elements $y \in Z_n$ satisfying $y^m = 1$.■

Theorem (1.6) *Let* p, q *be different primes,* $p > q$ *and* G *a group of order* pq*. Then one of the following holds*

- $G \cong Z_{pq}$*, or*
- $p \equiv 1 \pmod q$ *and* $G = Z_p Z_q$ *is a semidirect product with* Z_p *as normal subgroup.*

Proof: Let P be a p-Sylowsubgroup and Q a q-Sylowsubgroup. As $p > q$ and $[G : N_G(P)] \equiv 1 \pmod p$ we have $P \lhd G$. If in addition $Q \lhd P$, then $[P,Q] \subseteq P \cap Q = 1$. It follows that G is abelian, hence $G \cong Z_p \times Z_q = Z_{pq}$. So assume $Q \not\lhd G$. Then $N_G(Q) = Q$. By Sylow's theorem this can only happen if $p \equiv 1 \pmod q$. We have $G = PQ$ and Q operates on P by conjugation. Comparison with Definition (1.21) shows that G is isomorphic with the semidirect product.■

Problem (1.7) *Show that $E(4)$ and Z_4 are the only groups of order 4.*

Example (1.5) *Consider the symmetric group $S \cong S_n$ in its operation on $\Omega = \{1, \ldots, n\}$. One way of writing an element $g \in S$ is in the form*

$$g = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1g & 2g & \ldots & ng \end{pmatrix}$$

A handier way of writing g is as a product of cycles. Here a cycle $(a_1, a_2, \ldots, a_m)$ denotes the permutation $a_1 \longrightarrow a_2 \longrightarrow a_3 \longrightarrow \ldots \longrightarrow a_n \longrightarrow a_1$, which may best be visualized as a circle of length m. Each $g \in S$ is a product of disjoint cycles. These cycles are uniquely determined except for the choice of the starting point of a cycle, which is arbitrary. For example $(a_1, a_2, \ldots, a_m) = (a_2, \ldots, a_m, a_1)$. The cycles are the orbits of $< g >$ on Ω. Here is an example:

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 6 & 1 & 4 \end{pmatrix} = (1, 2, 5)(3)(4, 6).$$

This is a permutation of **cycle type** *$(1, 2, 3)$. Fixed points (cycles of length 1) are often omitted. In general the* **cycle type** *is a partition of the number n and gives the length of the cycles.*
Cycle notation facilitates calculation of conjugates. Let $g, h \in S$, where $g = \prod_{i=1}^{s}(a_{i1}, a_{i2}, \ldots, a_{i,r_i})$ (hence of cycle type $(r_1, r_2, \ldots, r_s)$). Then $g^h = \prod_{i=1}^{s}(a_{i1}h, a_{i2}h, \ldots, a_{i,r_i}h)$ As an example, use $g \in S_6$ above and $h = (1, 3)(2, 5, 4, 6)$. Then $g^h = (3, 5, 4)(1)(6, 2)$. In particular we see that conjugate permutations have the same cycle type. It is also clear that permutations with the same cycle type are conjugate in S_n.

Corollary (1.2) *The permutations of the same cycle type are the conjugacy classes of S_n. These are in bijection with the partitions of n.*

Definition (1.23) (transpositions) *A* **transposition** *is a cycle (a, b) of length 2. As $(a_1, a_2, \ldots, a_m) = (a_{m-1}, a_m)(a_{m-2}, a_{m-1}) \ldots (a_2, a_3)(a_1, a_2)$ each permutation is a product of transpositions.*

Definition (1.24) (signum) *Let $g \in S_n$, in its operation on $\Omega = \{1, 2, \ldots, n\}$. Fix a total ordering on $\Omega : 1 < 2, \ldots < n$. The* **signum** *$sgn(g)$ is the parity (± 1) of the number of pairs $\{i, j\}$ such that $i < j$ but $ig > jg$ (pairs changing orientation). It is clear that this notion does not depend on the total ordering chosen.*

Lemma (1.14) *We have $sgn(1) = 1$. If g is any permutation and t a transposition, then $sgn(gt) = -sgn(g)$.*

Proof: It is obvious that $sgn(1) = 1$. Let $t = (a, b)$, where $a < b$. The pairs whose orientation after application of g is different from that after application of gt are the following:

- $\{a, i\}$, where $a < i < b$,
- $\{b, i\}$, where $a < i < b$,
- $\{a, b\}$

As this is an odd number we are done.■

This shows that the permutations of signum $= +1$ are those which can written as a product of an even number of transpositions. Obviously these form a subgroup, even a normal subgroup, clearly of index 2 in S_n.

Definition (1.25) (alternate group) *The* **alternate group** *A_n consists of the permutations of signum $+1$ in S_n (the* **even permutations***). A_n is a normal subgroup of index 2 in S_n if $n \geq 2$.*

We have seen that cycles of odd length are even permutations, cycles of even length are odd permutations. Consider the cycle type of g. Then $g \in A_n$ if and only g has an even number of cycles of even length. For example, our permutation of type $(1, 2, 3)$ is not in A_6 as it has one cycle of even length. A permutation of type $(2, 4)$ is in A_6 as it has two cycles of odd length.

Lemma (1.15) *Any subgroup of index 2 is a normal subgroup.*

Proof: If $[G : H] = 2$, then $G = H \cup Hg$, hence $Hg = G - H = gH$. It follows from the Definition (1.6) that $H \lhd G$.■

Definition (1.26) (dihedral groups) *Consider the subgroup $D \leq S_n$ generated by $z = (1, 2, \ldots, n)$ and $x = (1, n)(2, n-1)\ldots = \prod_{i=1}^{\lfloor n/2 \rfloor}(i, n+1-i)$. We have $x^2 = 1, z^n = 1, z^x = z^{-1}$. In particular $< z > \lhd D =< z, x >$ is a normal subgroup of index 2 and D has order $2n$. We call $D = D_{2n}$ the*

dihedral group *of order* $2n$*. It may also described as a semidirect product* $Z_n \cdot Z_2$ *or as the group of symmetries of a circle of length* n*, where the cyclic subgroup* Z_n *represents the rotations and the remaining* n *elements operate as reflections.*

Example (1.6) (small permutation groups) *We have*
$A_2 = 1, S_2 \cong Z_2, A_3 =< (1,2,3) >\cong Z_3, S_3 =< (1,2,3) >< (1,2) >\cong D_6$.
$A_4 = V \cdot U$*, a semidirect product, where* $V =< (1,2)(3,4),(1,3)(2,4) > \lhd A_4, V \cong E(4)$ *and* $U =< (1,2,3) >\cong Z_3$.
$S_4 = A_4 < (1,2) >= V \cdot W$*, where* $W =< (1,2,3),(1,2) >\cong S_3 \cong D_6 \cong GL(2,2)$.

Theorem (1.7) A_5 *is the only simple group of order 60.*

Proof: Let us write down at first the conjugacy classes of S_5. These in bijection with the 7 partitions of the number 5. We obtain the following table:

number	representative	centralizer	length
1	id	S_5	1
2	(1,2,3,4,5)	¡(1,2,3,4,5)¿	24
3	(1,2,3)	$< (1,2,3)(4,5) >\cong Z_6$	20
4	(1,2)	$< (1,2) > \times S_3$	10
5	(1,2)(3,4)	$< (1,3,2,4),(1,2) >\cong D_8$	15
6	(1,2,3,4)	¡(1,2,3,4)¿	30
7	(1,2,3)(4,5)	$< (1,2,3)(4,5) >\cong Z_6$	20

The normal subgroup A_5 of order 60 consists of the union of conjugacy classes 1,2,3,5. Let $g \in A_5$. The orbit length formula from Lemma (1.9) shows the following: if$\mathbb{C}(g) \subseteq A_5$, then the conjugacy class g^{S_5} splits into two conjugacy classes of equal length in A_5. In the contrary case, when$\mathbb{C}(g) \not\subseteq A_5$, then $g^{S_5} = g^{A_5}$. Upon inspection of the Table we see that that A_5 has five conjugacy classes of lengths 1,12 (5-cycles),12 (5-cycles),20 (3-cycles),15 (products of two transpositions).
We prove at first that A_5 is a simple group. Assume $1 < N \lhd A_5$. Then N is a union of conjugacy classes of A_5. On the other hand $1 \in N$ $|N|$ must divide 60. This is impossible. We have seen that A_5 is a simple group.

Assume now G is a simple group of order 60. Sylow's theorem gives us $S \in Syl_2(G)$ of order 4, $P \in Syl_5(G), Q \in Syl_3(G)$. We know from Sylow's theorems that $[G : \mathbb{N}(P)] \equiv 1 \pmod 5$ and $\neq 1$ because of the simplicity of G. As $[G : \mathbb{N}(P)]|12$ we see that the only possibility is $[G : \mathbb{N}(P)] = 6$. We have therefore $|\mathbb{N}(P)| = 10$. An analogous argument shows $|\mathbb{N}(Q)| = 6$. We see already that G has 24 elements of order 5 and 20 elements of order 3. The order of 15 elements of G is still in doubt. It is impossible that $\mathbb{N}(P)$ or $\mathbb{N}(Q)$ are cyclic as this would lead either to 24 elements of order 10 or to 20 elements of order 6, which is impossible. We conclude from Theorem (1.6) that $\mathbb{N}(P)$ and $\mathbb{N}(Q)$ are semidirect products $Z_5 \cdot Z_2$ and $Z_3 \cdot Z_2$. As $Aut(Z_5) \cong Z_4$ and $Aut(Z_3) \cong Z_2$ each contain only one **involution** (= element of order 2), we see that the isomorphism types are uniquely determined. It follows $\mathbb{N}(P) \cong D_{10}, \mathbb{N}(Q) \cong D_6$. In particular G does not contain elements of orders 10 or 6. Let z be an involution in G. We have seen that $[G : \mathbb{C}(z)]$ is a multiple of 15. It follows that $\mathbb{C}(z)$ has order 4 and G has 15 involutions, which form a conjugacy class. In particular G does not contain elements of order 4. It follows that $S \cong E(4)$ and that any two different conjugates of S intersect trivially. This show that S has only 5 different conjugates, hence $[G : \mathbb{N}(S)] = 5$. Consider the representation of G by multiplication on the right cosets of $\mathbb{N}(S)$ (compare Example (1.4)). This is a transitive permutation representation of degree 5, hence a group homomorphism $\alpha : G \longrightarrow S_5$. We know that $ker(\alpha) \lhd G$. As G is simple it follows $ker(\alpha) = 1$, so that α is an isomorphism from G onto a subgroup of S_5. As G is simple and A_5 is simple we have $Im(\alpha) = Im(\alpha)' \subseteq S_5 = A_5$. It follows $Im(\alpha) = A_5$.■

Problem (1.8) *Show that there is no simple nonabelian group of order* < 60.

Definition (1.27) (composition series) *A* **composition series** (K) *of* G *is a chain of subgroups*

$$G = G_0 > G_1 > G_2 > \ldots > G_r = 1,$$

where $G_i \lhd G_{i-1}$ *and* G_{i-1}/G_i *is simple. The* **composition factors** *are factor groups* $G/G_1, G_1/G_2, \ldots, G_{r-1}$, r *is the length of* (K). *Composition series* $(K_1), (K_2)$ *are* **equivalent** *if the length and the composition factors are the same (including multiplicities).*

Theorem (1.8) (Jordan-Hölder) *If G possesses a composition series, then all composition series of G are equivalent (observe that finite groups do possess composition series).*

Proof: Let $(K_1) = (K)$ as in Definition (1.27) and

$$(K_2) : G = H_0 > H_1 > H_2 > \ldots > H_s = 1$$

be two composition series for G. Use induction on r (case $r = 1$ is equivalent with G being simple, and the claim is trivially true in that case). If $G_1 = H_1$, then we are done by induction. We can assume $G_1 \neq H_1$. It follows $G_1H_1 = G$. Put $L_2 = G_1 \cap H_1$. By the second isomorphism theorem (1.2) we have $G/G_1 \cong H_1/L_2$ and $G/H_1 \cong G_1/L_2$ and both groups are simple. Let (L) be a composition series of L_2. Then (K_1) is equivalent with $G > G_1 > L_2 > (L)$, which is equivalent with $G > H_1 > L_2 > (L)$. As this composition series is equivalent with (K_2) we conclude that (K_1) and (K_2) are equivalent.■

Definition (1.28) (solvable groups) *A group G is* **solvable** *if every composition factor has prime order.*

Observe that simple groups either have prime order or are nonabelian. The following facts are trivial: If G is solvable, then all subgroups and all factor groups of G are solvable. If $N \lhd G$ is solvable and G/N is solvable, then G is solvable. We conclude from Theorem (1.5) that p-groups are solvable. It is easy to see that $N_1 \lhd N_2 \lhd G$ does not in general imply that N_1 is a normal subgroup of G (the group A_4 furnishes examples). It is therefore interesting to find a property, which is stronger than the normal subgroup property and is transitive.

Definition (1.29) (characteristic subgroups) *A subgroup $H \leq G$ is a* **characteristic subgroup** *(H char G) if we have $H\alpha = H$ for all $\alpha \in Aut(G)$.*

Lemma (1.16) *The following hold:*

- *If H char G, then $H \trianglelefteq G$.*

- *If* H_1 *char* H_2 *char* G, *then* H_1 *char* G.

- *If* H *char* $N \trianglelefteq G$, *then* $H \trianglelefteq G$.

Proof: Observe that the condition on $N \leq G$ to be a normal subgroup as given in Definition (1.6) may equivalently be written as follows: every inner automorphism of G maps N onto itself (see Definition (1.14)). If $g \in G$ and $N \trianglelefteq G$, then conjugation indices an automorphism on N. All the statements of the Lemma follow from these remarks.∎

Example (1.7) *Obvious examples of characteristic subgroups of* G *are* $\mathbb{Z}(G), G'$ *as well as the following:*

- $O_p(G)$, *the largest normal subgroup, which is a p-group,*

- $O^p(G)$, *the smallest normal subgroup such that the factor group is a p-group,*

- $G'(p)$, *the smallest normal subgroup such that the factor group is an abelian p-group.*

1.1 Transfer and fusion

Definition (1.30) (fusion) *Let $H \leq G$ and $A, B \subseteq H$. Write $A \sim_H B$ if there exists $h \in H$ such that $A^h = B$. We call A and B* **fusioned** *in G if $A \not\sim_H B$ but $A \sim_G B$.*

Transfer is an important means to prove fusion theorems. We start with some easy cases without using transfer. Remember that elements of order 2 are called **involutions**.

Theorem (1.9) (Thompson) *Assume G does not contain a (normal) subgroup of index 2 (equivalently $O^2(G) = G$). Let M be a maximal subgroup of $S \in Syl_2(G)$. Then every involution in G is conjugate to some involution in M.*

Proof: We have $[G : M] = 2u$, where u is odd. Consider the permutation representation of G on the right cosets of M. Let $z^2 = 1$, assume z is not conjugate under G to some element of M. Then z does not fix any coset of M as otherwise $Mg = Mgz$ for some g, which leads to the contradiction $gzg^{-1} \in M$. It follows that z is the product of u transpositions, hence $z \notin A_{2u}$. Consequently $G \cap A_{2u}$ is a subgroup of index 2 in G, contradiction.∎

Theorem (1.10) (Burnside) *Let $P \in Syl_p(G)$ and A, B normal subsets (= unions of conjugacy classes) of P. Then the following holds:*

$$A \sim_G B \text{ if and only if } A \sim_{\mathbb{N}_G(P)} B.$$

Proof: Let $A^g = B$. Then $N = \mathbb{N}(B)$ contains P and P^g. By Sylow's theorem, applied to N, we see that there is some $h \in N$ such that $P = P^{gh}$, hence $gh \in \mathbb{N}_G(P)$ and $A^{gh} = B^h = B$.∎

Definition (1.31) (transversals) *Let $H \leq G, [G : H] = n$. A* **right transversal** *is a set $T = \{t_1, t_2, \ldots, t_n\}$ of representatives of the distinct right cosets of H in G. A* **left transversal** *is defined analogously. Let T be a right transversal, $t \in T, x \in G$. Then $Htx = Ht'$ for some $t' \in T$. In particular $tx = ht'$, where $h \in H$ and $t' \in T$ are uniquely determined. We define functions*

$$\alpha_x^T : T \longrightarrow H, \phi_x^T : T \longrightarrow T$$

by $tx = (t\alpha_x^T)(t\phi_x^T)$.

Definition (1.32) (transfer) *Let $H \leq G, [G : H] = n < \infty, T$ a right transversal of H in G and $H' \leq K \leq H$. The* **transfer** *$V = V_{G \longrightarrow H/K}$: $G \longrightarrow H/K$ is defined by*

$$xV = K \prod_{t \in T} (t\alpha_x^T).$$

Lemma (1.17) *Let $H \leq G, T$ a right transversal and $V = V_{G \longrightarrow H/K}$ the transfer. Then V is independent of the choice of right transversal and V is a homomorphism $V : G \longrightarrow H/K$.*

Proof: As the image of V is contained in the abelian group H/K we can reorder at our ease. At first we prove the independence. So let S be an arbitrary right transversal, $s = h_t t \in S$, where $h_t \in H$. We have $sx = (h_t t)x = h_t(t\alpha_x^T)(t\phi_x^T) = h_t(t\alpha_x^T)h_{t\phi_x^T}^{-1}s'$ where $s' \in S$. It follows $s\alpha_x^S = h_t(t\alpha_x^T)h_{t\phi_x^T}^{-1}$. Clearly ϕ_x^T is a permutation of T. In the product, taken mod K, the h-factors cancel.
Fix T now. We wish to show that V is a group homomorphism. We have $txy = (t\alpha_{xy})(t\phi_{xy}) = (tx)y = (t\alpha_x)(t\phi_x)y = (t\alpha_x)(t\phi_x\alpha_y)(t\phi_x\phi_y)$. We conclude

$$t\alpha_{xy} = (t\alpha_x)(t\phi_x\alpha_y) \tag{1.1}$$
$$t\phi_{xy} = t\phi_x\phi_y \tag{1.2}$$

It follows $xyV = K\prod_{t\in T}(t\alpha_x(t\phi_x)\alpha_y$. As ϕ_x affords a permutation of T it follows that $xyV = (xV)(yV)$. Inverses are treated in an analogous way.∎

Given $x \in G$ we can choose a transversal adapted to x. Assume the operation of x on G/H has cycle type $(r_1, r_2, \ldots, r_t)$. Let $x_i \in G, i = 1, 2, \ldots t$ be a representative of a right coset belonging to the i-th orbit. Choose as transversal

$$T = \cup_{i=1}^t \{x_i = t_{i,0}, x_i x = t_{i,1}, \ldots, x_i x^{r_i - 1} = t_{i,r_i-1}\}.$$

In particular $t_{i,j}\alpha_x = 1$ when $j < r_i - 1$. Further $t_{i,r_i-1}x = x_i x^{r_i} = (x_i x^{r_i} x_i^{-1})x_i$. It follows

$$t_{i,r_i-1}\alpha_x = x_i x^{r_i} x_i^{-1} \in H$$

and $t_{i,r_i-1}\phi_x = x_i$. This leads us to the following Theorem:

Theorem (1.11) *Let $H \leq G, [G : H] = n < \infty$ and $x \in G$. Let the cycle type of x in its multiplication operation on the right cosets of H be $(r_1, r_2, \ldots, r_t)$ (in particular $\sum_{i=1}^{t} r_i = n$). Then there are elements $x_i \in G, i = 1, 2, \ldots, t$ such that $x_i x^{r_i} x_i^{-1} \in H$ and*

$$xV_{G \longrightarrow H/K} = \prod_{i=1}^{t} x_i x^{r_i} x_i^{-1}.$$

We see that this is related to fusion: the r_i-th power of x is conjugate under G to some element of H.

Definition (1.33) (D.G. Higman) *Let $H \leq G, [G : H] < \infty$. The* **focal subgroup** *is defined as*

$$Foc_G(H) = H_G^* = H^* =< h^{-1}h^g = [h, g] | h \in H, g \in G, h^g \in H > .$$

Clearly we have $H' \leq Foc_G(H) \leq H$. In particular we may use $K = Foc_G(H)$ in the Definition of the transfer. The case when $H = P \in Syl_p(G)$ and $K = P^*$ is the focal subgroup is of particular interest.

Lemma (1.18) *Let $[G : H] = n, V = V_{G \longrightarrow H/K}$, where $H^* \leq K \leq H$. Then the following hold:*

- *If $h \in H$, then $hV = Kh^n$.*
- *If $gcd([H : K], n) = 1$, then the restriction of V is surjective and $H \cap ker(V) = K$.*

Proof: By definition of $H^* = Foc_G(H)$ we have $Kh = Kh^g$ whenever $h \in H, g \in G, h^g \in H$. By Theorem (1.11) we have $hV = K \prod_{i=1}^{t} h^{r_i} = Kh^n$. The rest is clear as raising to the n-th power is a group isomorphism in an abelian group whose order is coprime to n. ∎

Theorem (1.12) (D.G. Higman) *Let $P \in Syl_p(G), P^* = Foc_G(P)$. Then the following hold:*

- *$P^* = P \cap G'$.*

- $G/G'(p) \cong P/P^*$.

Proof: By definition of $G'(p)$ we have $G = PG'(p)$. It follows from the second isomorphism theorem that $G/G'(p) \cong P/(P \cap G'(p))$. It follows from the Definition that $P^* \leq P \cap G'$. Lemma (1.18) shows that $V : G \longrightarrow P/P^*$ is surjective and that $ker(V) \cap P = P^*$. As $G/ker(V) \cong P/P^*$ is an abelian p-group we have $ker(V) \geq G'(P) \geq G'$. We get $P^* \leq P \cap G' \leq P \cap G'(p) \leq P \cap ker(V) = P^*$. We have equality all the way. The claims follow.■

Harmless as it looks this Theorem is an important insight. It says that the factor group $G/G'(p)$ is determined by the following data:

1. The isomorphism type of $P \in Syl_p(G)$, and
2. the fusion of elements in P under G.

As a Corollary we obtain an important result of Burnside's:

Theorem (1.13) (Burnside) *Let $P \in Syl_p(G)$. Assume $\mathbb{C}_G(P) = \mathbb{N}_G(P)$. Then G has a* **normal p-complement.** *This is a normal subgroup $N \lhd G$ such that $N \cap P = 1$ and $NP = G$.*

Proof: It follows from the assumption that P is abelian. It follows from Theorem (1.10) that fusion in P is controlled by $\mathbb{N}_G(P)$. The assumption says that there is no such fusion, or equivalently $Foc_G(P) = 1$. It follows from Theorem (1.12) that $G/G'(p) \cong P$. The kernel of the transfer map is a normal p-complement.■

Corollary (1.3) *Let G be a group of even order, $S \in Syl_2(G)$. If S is cyclic, then G has a normal 2-complement.*

Proof: Let S be cyclic of order 2^a. We have $|Aut(S)| = \phi(2^a) = 2^{a-1}$ (see Lemma (1.13)). Moreover we know that $\mathbb{N}_G(S)/\mathbb{C}_G(S)$ is isomorphic with a subgroup of $Aut(S)$ (see Lemma (1.8)). As this is a group of odd order, we conclude $\mathbb{N}_G(S) = \mathbb{C}_G(S)$. Use Theorem (1.13). ■

Chapter 2

Elementary Theory of permutation groups

Definition (2.1) *Permutation groups* (G,Ω) *and* (H,Ω') *are* **equivalent** *if there is an isomorphism* $\alpha : G \longrightarrow H$ *and a bijection* $\beta : \Omega \longrightarrow \Omega'$ *such that*

$$(xg)\beta = (x\beta)(g\alpha) \text{ for all } x \in \Omega, g \in G.$$

Lemma (2.1) *Let* (G,Ω) *be transitive. Then* (G,Ω) *is equivalent with the multiplication representation of* G *on* G/G_x.

Proof: We know that $|\Omega| = |G/G_x|$ (see Lemma (1.9)). Let α be the identity and $\beta : G/G_x \longrightarrow \Omega$ the canonical mapping $G_x g \mapsto xg$. ∎

We see that transitive permutation representations can be found inside the group. They correspond simply to subgroups.

Lemma (2.2) (Burnside's Lemma) *Let* (G,Ω) *be a permutation group. Then the following hold:*

1. *If* G *has* t *orbits on* Ω, *then*

$$t|G| = \sum_{g\in G} |F(g)| (\textbf{Burnside'sLemma})$$

2. *Let G be transitive ($t = 1$) and let G_x have r orbits on Ω. Then r (the* **rank** *of (G, Ω)) is independent of the choice of $x \in \Omega$ and we have*

$$r \cdot |G| = \sum_{g \in G} |F(g)|^2.$$

Proof: 1. Count pairs (g, x), where $g \in G, x \in \Omega, xg = x$ in two ways. This yields $\sum_{x \in \Omega} |G_x| = \sum_{g \in G} |F(g)|$. If Δ is an orbit, then for every $x \in \Delta$ we have $|G_x| = |\Delta|/|\Delta|$, by Lemma (1.9). It follows $\sum_{x \in \Delta} |G_x| = |G|$. Claim 1. follows.
2. We know from part 1. that $r \cdot |G_x| = \sum_{g \in G_x} |F(f)|$. For $x, y \in \Omega$ we have that (G_x, Ω) and (G_y, Ω) are equivalent. In fact, pick an element $g \in G$ such that $xg = y$. The equivalence (see Definition (2.1)) may defined by $\alpha : h \mapsto h^g$ and $\beta : z \mapsto zg$ (if $h \in G_x$, then $yh^g = (xg)g^{-1}hg = xhg = xg = y$). It follows that r is independent of the choice of x. We calculate $r \cdot |\Omega| \cdot r \cdot G \cdot = \sum_{x \in \Omega} \sum_{g \in G_x} |F(g)| = \sum_{g \in G} \sum_{x \in F(g)} |F(g)| = \sum_{g \in G} |F(g)|^2$. ■
Burnside's Lemma says that in the transitive case the average number of fixed points of a group element is 1. As the identity has more than 1 fixed point it follows in particular that there most be fixed-point-free elements.

Corollary (2.1) *If the permutation group (G, Ω) is transitive, $|\Omega| > 1$, then there exists an element $g \in G$ such that $F(g) = \emptyset$.*

Definition (2.2) *(G, Ω) is t-***transitive** *($t \geq 1$) if whenever two t-tuples $(x_1, x_2, \ldots, x_t)$ and $(y_1, y_2, \ldots, y_t)$ of different elements in Ω are given, there exists $g \in G$ such that $x_i g = y_i, i = 1, 2, \ldots, t$ (the x_i have to be pairwise different, also the y_i are pairwise different; nothing is assumed about the relation between the x_i and the y_j).*

It is clear that 1-transitivity is equivalent with transitivity and that t-transitivity implies $(t-1)$-transitivity $(t > 1)$. One may also say that (G, Ω) is t-transitive if and only if G is transitive in its implied operation on t-tuples of pairwise different elements from Ω. The proof of the following Lemma is formal and trivial:

Lemma (2.3) *Let (G, Ω) be a permutation group. Then the following are equivalent:*

- (G, Ω) *is* t*-transitive* $(t \geq 1)$.

- (G, Ω) *is transitive and* $(G_x, \Omega - \{x\})$ *is* $(t-1)$*-transitive.*

- (G, Ω) *is* $(t-1)$*-transitive and for some (all)* $(t-1)$*-tuple* $(x_1, \ldots, x_{t-1})$ *we have that* $(G_{(x_1,\ldots,x_{t-1})}, \Omega - \{x_1, \ldots, x_{t-1}\})$ *is transitive. Here* $G_{(x_1,\ldots,x_{t-1})}$ *denotes* $\cap_{i=1}^{t-1} G_{x_i}$.

Corollary (2.2) *If* (G, Ω) *is* t*-transitive,* $|\Omega| = n$*, then* $|G| = n(n-1) \cdot \ldots (n-t+1)|G_{(x_1,\ldots,x_t)}|$.

Proof: This follows by repeated application of Lemma (1.9).■

Problem (2.1) *Let* $A, B \leq G$*. Then* $|AB| = |A| \cdot |B|/|A \cap B|$.

Definition (2.3) (double cosets) *Let* $H, K \leq G$*. A set* HgK *for some* $g \in G$ *is called a* **double coset** *of* G *for* H *and* K*. Observe that* HgK *is a union of right cosets for* H *and a union of left cosets for* K.

Lemma (2.4) *Let* $H, K \leq G$*. The following hold:*

1. *If* $x \in HgK$*, then* $HxK = HgK$.

2. G *is the disjoint union of its different double cosets for* H *and* K.

3. HgK *is the union of* $|K|/|H^g \cap K|$ *right cosets for* H *and of* $|H|/|H^g \cap K|$ *left cosets for* K.

Proof: 1. $HhgkK = HgK$.
2. follows from 1.
3. $|HgK| = |g^{-1}HgK| = |H^gK| = |H^g| \cdot |K|/|H^g \cap K| = |H| \cdot |K|/|H^g \cap K|$.
The second formula follows in an analogous way.■

Lemma (2.5) *If* (G, Ω) *is 2-transitive,* $g \notin G_x$*, then* $G = G_x \cup G_x g G_x$ *is the union of two double cosets for* G_x.

Proof: Consider g as fixed, choose $g' \in G - G_x$. Because of double transitivity there is some $h \in G_x$ such that $G_x g' = G_x gh$. It follows $g' \in G_x g G_x$. Here we have used Lemma (2.1).■

Example (2.1) *The symmetric group S_n is clearly n-transitive. The alternating group A_n is $(n-2)$-transitive $(n \geq 3)$. For $n = 3$ this is clear. For general n it follows by induction as the stabilizer of a point in A_n is A_{n-1}.*

Definition (2.4) (primitivity) *Let (G, Ω) be transitive. Let $\Delta \subset \Omega, |\Delta| > 1$. Δ is a* **region of imprimitivity** *of (G, Ω) if for every $g \in G$ either $\Delta g = \Delta$ or $\Delta g \cap \Delta = \emptyset$. Call (G, Ω)* **primitive** *if it does not contain a region of imprimitivity.*

If $\Delta \subset \Omega$ is a region of imprimitivity, $|\Omega| = n, |\Delta| = m$, then clearly $m|n$ and the number of distinct images of Δ is n/m. We view the permutation representation of G on Ω as composed out of a representation on n/m points (the images of Δ) and a representation of the stabilizer of Δ on Δ.

Theorem (2.1) *Let (G, Ω) be transitive. Then (G, Ω) is primitive if and only if the stabilizer G_x of some (any) $x \in \Omega$ is a* **maximal subgroup** *of G. Here we call $H \leq G$ a maximal subgroup if there is no subgroup L such that $H < L < G$.*

Proof: 1. Let $\Delta \subset \Omega$ be a region of imprimitivity, denote by G_Δ the stabilizer of Δ. By definition of we have for every $x \in \Delta$ that $G_x \subseteq G_\Delta$. As $|\Delta| > 1$ we have $G_x \neq G_\Delta$. As $\Delta \neq \Omega$ we have $G_\Delta \neq G$.
2. Assume $G_x < H < G$. Put $\Delta = xH$. Then Δ is a region of imprimitivity, and $|\Delta| = [H : G_x]$.■

Theorem (2.2) *If (G, Ω) is 2-transitive, then (G, Ω) is primitive.*

Proof: Let $\Delta \subset \Omega$ be a region of imprimitivity. Choose $x, y \in \Delta, x \neq y$ and $z \notin \Delta$. By definition of 2-transitivity we find $g \in G$ such that $xg = x, yg = z$. This contradicts the definition of a region of imprimitivity.■

2.1 Normal subgroups and permutation representations

Theorem (2.3) *If (G, Ω) is primitive and $1 \neq N \lhd G$, then (N, Ω) is transitive.*

Proof: Let $|\Omega| = n$. We have $G_x \leq G_x N \leq G$ (see Lemma (1.6)). Because of primitivity we have either $G_x N = G$ or $G_x N = G_x$. Assume $G_x N = G_x$, equivalently $N \leq G_x$. By conjugation we see that $N \leq G_y$ for all $y \in \Omega$, hence $N = 1$, contradiction. We conclude $G_x N = G$. As

$$n = |G|/|G_x| = |N|/|G_x \cap N|,$$

we conclude that N is transitive on Ω.■

Definition (2.5) *(G, Ω) is* **sharply t-transitive** *($t \geq 1$) if whenever two t-tuples $(x_1, x_2, \ldots, x_t)$ and $(y_1, y_2, \ldots, y_t)$ of different elements in Ω are given, there exists exactly one $g \in G$ such that $x_i g = y_i, i = 1, 2, \ldots, t$.*
(G, Ω) is **regular** *if it is sharply 1-transitive, equivalent if (G, Ω) is transitive and $|G| = |\Omega|$.*

Theorem (2.4) *Let (G, Ω) be primitive and G_x a simple group. Then one of the following holds:*

- *Either G is simple, or*
- *G contains a normal subgroup N such that (N, Ω) is regular.*

Proof: Assume G is not simple. Let $1 \neq N \lhd G$. We know from Theorem (2.3) that (N, Ω) is transitive. We have to show that $N \cap G_x = 1$. As G_x is a simple group and $N \cap G_x \trianglelefteq G_x$ the only other possibility is $N \cap G_x = G_x$, equivalently $G_x \leq N$. It follows from Lemmaorbitlengthlemma that $N = G$, contradiction.■

So we can sometimes guarantee the existence of a normal regular subgroup. Let us study this situation more in detail.

Lemma (2.6) *Let (G,Ω) be transitive, $N \lhd G$ such that (N,Ω) is regular. Then $(G_x, \Omega - \{x\})$ is equivalent with the representation of G_x by conjugation on $N - \{1\}$.*

Proof: Observe that $x \in \Omega$ is fixed. In the terminology of Definition (2.1) we choose $\alpha : G_x \longrightarrow G_x$ to be the identity.

$$\beta : \Omega - \{x\} \longrightarrow N - \{1\}$$

is defined as $y\beta = n \in N$ satisfying $xn = y$. Observe that $n \neq 1$ exists and is uniquely determined as N is regular on Ω. Thus β certainly defines a bijection. We have to check the defining property of equivalence. Let $h \in G_x, y \in \Omega - \{x\}$. We need to show that $(yh)\beta = h^{-1}(y\beta)h$. Put $(yh)\beta = n, y\beta = n'$. Then $xn = yh$ and $xn' = y$. It follows $x(h^{-1}n'h) = xn'h = yh$. This shows $n = h^{-1}n'h$, as claimed.■

We can interpret Lemma (2.6) as saying that for every choice of $x \in \Omega$ the set Ω can be given a group structure, with x in the role of the neutral element and G_x respects this group structure.■

We obtain a first classification theorem:

Theorem (2.5) *Let (G,Ω) be t-transitive ($t \geq 2$) with a regular normal subgroup N. Then $t < 5$ and one of the following holds:*

1. *$t = 2, N \cong E(p^n)$ for some prime p.*
2. *$t = 3$ and either $N \cong Z_3$ or $N \cong E(2^n)$.*
3. *$t = 4, N \cong E(4)$.*

Proof: It follows from Lemma (2.6) that the automorphism group of N is $(t-1)$-transitive on $N - \{1\}$. Certainly $t \geq 2$. The transitivity shows that N must be elementary abelian of some prime-power order. If $t = 3$, then the double transitivity shows that either $N \cong Z_3$ or $p = 2$. If $t > 3$, then clearly $N \cong E(4)$ and $t = 4$. ■

As a consequence of this theory we obtain an easy proof for the fact that the alternating groups are simple groups:

Theorem (2.6) *The alternating groups A_n are simple when $n \geq 5$.*

Proof: We have shown in Theorem (1.7) that A_5 is simple. Let now $n > 5$. The stabilizer of a point in A_n is A_{n-1}. By induction we can assume that A_{n-1} is a simple group. A_n is highly transitive, hence certainly primitive. If A_n is not simple, then we know from Theorem (2.4) that A_n must contain a regular normal subgroup. By Theorem (2.5) this implies $t \leq 4$, hence $n = 6$. By Theorem (2.5) we get a contradiction even in case $n = 6$.■

2.2 Transitive extensions and the small Mathieu groups

Let (G, Ω) be a transitive permutation group. We have studied the corresponding operation $(G_x, \Omega - \{x\})$ of the stabilizer. We ask under which conditions this process can be reversed. So let (H, Ω) be given. Can we find $(G, \Omega \cup \{*\})$ such that $G_* = H$? If (H, Ω) is t-transitive, then necessarily $(G, \Omega \cup \{*\})$ will be $(t+1)$-transitive. We study the case when $t \geq 2$. Let $x, y \in \Omega, x \neq y$. Pick a permutation g of $\Omega \cup \{*\}$ affording the operation $g : * \longleftrightarrow x, y \longleftrightarrow y$ and $h \in H$ such that $h : x \longleftrightarrow y$. Let $f \in H_x$. Then gfg fixes $*$ and x. It follows $gH_xg = H_x$. We will see that these conditions suffice to define a transitive extension.

Theorem (2.7) (transitive extension) *Let (H, Ω) be t-transitive for some $t \geq 2$. Put $\Omega^* = \Omega \cup \{*\}$. Assume we can find a permutation g of Ω^* and an element $h \in H$ such that the following hold:*

1. *$g : * \longleftrightarrow x, h : x \longleftrightarrow y, yg = y$.*

2. *g^2 and $(hg)^3$ are in H.*

3. *$gH_xg = H_x$.*

Then $G =< H, g >= H \cup H \cdot g \cdot H$ is $(t+1)$-transitive on Ω^* and $G_* = H$.

Proof: By assumption we have h and the new permutation g operating on the set $\{*, x, y\}$. Observe that it suffices to prove that the union $H \cup HgH$ is a group. The remaining claims follow automatically (for example this group operates on Ω^*, the element $*$ is not fixed and H is the stabilizer of $*$. As H is t-transitive, it follows that G must be $(t+1)$-transitive). Let us prove this fact. As H is a group it suffices to show that $gHg \subseteq H \cup HgH$. We use the 2-transitivity of H. By Lemma (2.5) $H = H_x \cup H_x h H_x$. It is one of our assumptions that $gH_x g = H_x$. Remains to show that $gH_x h H_x g \subseteq HgH$. This is the case: $(gH_x)h(H_x g) = (H_x g)h(gH_x) \subseteq H_x(hgh)HH_x \subseteq HgH$. Here we have used the assumptions, in particular that $(hg)^3 \in H$.■

We are going to construct some particularly interesting permutation groups, the small Mathieu groups:
Let $Z = \{a, b, c, d, e, f\}$ be a 6-set and G the group of permutations of Z. The order of G is $6! = 10 \cdot 9 \cdot 8$. The group G also operates on the $\binom{6}{3}/2$ complementary pairs of 3-subsets of Z. These form our set $\Omega = \{0, 1, \ldots, 9\}$, where

$0 = (abc\|def)$	$1 = (abd\|cef)$
$2 = (abe\|cdf)$	$3 = (abf\|cde)$
$4 = (acd\|bef)$	$5 = (ace\|bdf)$
$6 = (acf\|bde)$	$7 = (ade\|bcf)$
$8 = (adf\|bce)$	$9 = (aef\|bcd)$

We see G as a subgroup of the symmetric group on 10 objects now, without changing notation (the correct approach would be to speak of an embedding of S_6 into S_{10} and use a different symbol for the image of this embedding). Clearly G is faithful and transitive on 10 objects. Let $\phi_1 = (abc), \phi_2 = (bcd)$. These are permutations of order 3. Both stabilize object 0. In the operation on 10 points we have

$$\phi_1 = (1,9,4)(2,8,5)(3,7,6), \phi_2 = (1,2,3)(4,5,6)(7,9,8).$$

It is checked right away that ϕ_1, ϕ_2 commute. In particular we have that $E =< \phi_1, \phi_2 >$ is elementary abelian of order 9. We also see that E is transitive on $\Omega - \{0\}$. As $|G| = 10 \cdot 9 \cdot 8$ it follows that the stabilizer $G_{0,1}$ of two points has order 8. It is now clear that $G_{0,1} =< (a,b),(e,f),(a,e)(b,f)(c,d) >$. As this group has orbits $\{2,3,4,9\}$ and $\{5,6,7,8\}$ we see in particular that G is not 3-transitive on Ω.
Consider the normal subgroup $H < G$, where H is the alternate group on 6

objects. It is clear that H is transitive on 10 points. As $E < H$ it follows that H is 2-transitive on 10 points. It follows that $H_{0,1}$ has order 4. We see that $H_{0,1} =< \theta >$ is cyclic of order 4, where

$$\theta = (a, f, b, e)(c, d) = (2, 9, 3, 4)(5, 8, 7, 6).$$

It follows that $H_0 =< \phi_1, \phi_2, \theta >$ (of order 36). Put $\psi = (a, b)(c, d) = (01)(49)(56)(78)$. Then $H =< \phi_1, \phi_2, \theta, \psi >$.
Our next aim is to embed H in a group, which is double as large as H (contains H as a subgroup of index 2) and is 3-transitive on 10 points. To this end consider the permutation

$$\lambda = (2735)(4698).$$

Clearly λ is not in H, as it would have to be a power of θ otherwise. We have $\lambda^2 = \theta^2 \in H$. It is easy to check that λ normalizes H. If we denote conjugation by $\alpha^\beta = \beta^{-1}\alpha\beta$, then we have in fact

$$\phi_1^\lambda = \phi_1\phi_2, \phi_2^\lambda = \phi_1\phi_2^{-1}, \theta^\lambda = \theta^{-1}, \psi^\lambda = \psi\theta.$$

Put $M_{10} =< H, \lambda >$. We know that M_{10} contains H as a subgroup of index 2, hence has the same order $6! = 10 \cdot 9 \cdot 8$ as S_6. The operation of λ shows that M_{10} is 3-transitive, hence sharply 3-transitive. Next we construct a transitive extension of M_{10} : put $\Omega^* = \Omega \cup \{T\}$ and consider the permutation $g = (0, T)(4, 7)(5, 9)(6, 8)$. Then $g : T \longleftrightarrow 0, 1 \longleftrightarrow 1$ and $\psi : 0 \longleftrightarrow 1$. In order to be able and apply Theorem (2.7) we have to check that $g(M_{10})_0 g = (M_{10})_0$. As g is an involution this is equivalent to saying that g normalizes $(M_{10})_0$. As $(M_{10})_0$ contains H_0 and has order $9 \cdot 8$ it is clear that $(M_{10})_0 =< \phi_1, \phi_2, \theta, \lambda$. By the way, E is a normal subgroup of $(M_{10})_0$ and a Sylow-2-subgroup is $, \theta, \lambda >$. It is easily checked that this latter group is a quaternion group.
It is now clear that the conditions of Theorem (2.7) are satisfied. The group $M_{11} =< M_{10}, g >$ is sharply 4-transitive, of order $11 \cdot 10 \cdot 9 \cdot 8$. A Sylow-2-subgroup is $< \theta, \lambda, g >=< g\theta, g >$. Here $g\theta = (T, 0)(2, 9, 8, 5, 3, 4, 6, 7)$ has order 8, g is an involution and $(g\theta)^g = (g\theta)^3$. This group is known as **semidihedral group** (of order 16).

Lemma (2.7) *M_{11} is a simple group.*

Proof: Assume N is a nontrivial normal subgroup of $G = M_{11}$. It follows from Theorem (2.3) that N operates transitively. As a group of order 11 on 11 points has a normalizer of order 110 in S_{11}, it follows that $|N|N > 11$. In particular $N \cap M_{10}$ is a nontrivial normal subgroup of M_{10}. Remember that M_{10} was constructed as an extension of the simple group A_6 by a nontrivial automorphism. It follows that M_{10} has the group H (isomorphic with A_6) as only nontrivial normal subgroup. If $N \supset M_{10}$, then $N = M_{11}$, contradiction. It follows $N \cap M_{10} = H$. We conclude that N has index 2 in M_{11}. The Sylow theorem will give a contradiction: let P be a Sylow-11-subgroup of N (and of M_{11}). The Sylow theorem states that all Sylow-11-subgroups are conjugate and their number (= index of the stabilizer) is $\equiv 1 \pmod{11}$. We apply this to N and to M_{11}. This leads to a contradiction.∎

Here is another transitive extension: put $\Omega^{**} = \Omega \cup \{T, E\}$. Let $g' = (E,T)(2,9)(3,4)(5,7)$. We can choose g as its partner in M_{11} and see that $M_{12} =< M_{11}, g' >$ is sharply 5-transitive, of order $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$, of course.

Lemma (2.8) *M_{12} is a simple group.*

Proof: If M_{12} is not simple, then by Theorem (2.4) it must contain a regular normal subgroup N. The number of elements of order 3 in N is certainly < 11 then. Consider the operation of the simple group M_{11} by conjugation. It will have to operate trivially. In particular we find an element of order 3, which centralizes a group M_{11}. This is impossible.∎

Chapter 3

Polya's enumeration theory

Many combinatorial enumeration problems can be formulated as the determination of the number of orbits of a certain permutation group. As motivational examples let us consider the following two problems:

1. In how many essentially different ways can the six faxes of a die be colored with two colours (red and green, say) ? Here two colourings are equivalent if one can be obtained from the other by application of a rotation to the die (reflections are not allowed, and it is not allowed to change the role of the colours).

2. What is the number of essentially different graphs on five vertices? Here we consider only simple graphs (no loops, no multiple edges, no directed edges). Two graphs are equivalent if one can be obtained from the other by a permutation of the set of vertices.

At first we want to see that both problems belong to the same general family of enumeration problems, which may be described as follows:
Let G be a group operating on the set Ω. Denote by C^Ω the set of all mappings $\chi : \Omega \longrightarrow C$. Determine the number of orbits of G in its operation on C^Ω.
This needs some explanation. We may interpret the set C^Ω of all mappings $: \Omega \longrightarrow C$ as the set of all **colorings** of Ω with $|C|$ colours. Moreover it should be explained what the natural action of G on C^Ω is.

Lemma (3.1) *Let the group G act on the set Ω. The natural action of G as a group of permutations on the set C^Ω of all mappings $: \Omega \longrightarrow C$ (colorings)* *is defined as follows:*

$$x(\chi g) = (xg^{-1})\chi.$$

Here $\chi : \Omega \longrightarrow C, x \in \Omega, g \in G$. *This defines the image* χg *of the mapping* χ *under* g.

It is clear that for every $g \in G$ this defines a permutation of the colorings. If the coloring Ψ is given, the coloring χ defined by $y\chi = (yg)\Psi$ satisfies $\chi g = \Psi$. Moreover we see that the mapping $\chi \mapsto \chi g$ defines a permutation representation of G on the set C^Ω of colorings of Ω. In fact, we have $x\chi(g_1g_2) = (x(g_1g_2)^{-1})\chi = (xg_2^{-1}g_1^{-1})\chi$ and $x(\chi g_1)g_2 = (xg_2^{-1})\chi g_1 = (xg_2^{-1}g_1^{-1})\chi$. We obtain the same result. This shows that we have a permutation representation of G on the set of colorings.
In the first problem above choose G to be the group of all rotations in 3-space mapping the die (the cube) onto itself. We will see that G has order 24 and is isomorphic with the symmetric group S_4. We choose C to have 2 elements. The number we have to determine is the number of orbits of G on the set of colorings of the six faces of the die with 2 colours. We are talking about the permutation representation of G on the $2^6 = 64$ colorings of the faces induced by the permutation representation of G on the 6 faces, and we have to determine the number of vertices.
For the second problem above, we start from the symmetric group S_5, in its natural action on a 5-set V (the set of vertices of our graphs). Then $\Omega = \binom{F}{2}$ is the set of all unordered pairs of vertices. A graph is determined by deciding for every pair of vertices of they are joined by an edge or not. We may choose $C = \{e, n\}$, where e stands for **edge** and n for **nonedge.** There are clearly precisely $2^{10} = 1024$ such graphs. Two such graphs are equivalent if they are in the same orbit under the action of $G = S_5$. Again we have to determine the number of orbits.

In order to be able and solve the first problem we have to determine the group G of rotations of 3-space, which map the cube to itself. We denote the vertices as $P_1, \dots, P_8$ and the faces $F_1, \dots, F_6$. Here we use the convention that the indices of opposite faces add up to 7 (see the figure). It is clear that G is transitive on vertices, on edges and also on faces. The stabilizer of a face is a cyclic group of order 4. For example, the stabilizer of F_1 is generated by the rotation about the axis through the centers of F_1 and F_6

by the angle $\pi/2$, hence $G_{F_1} =< \alpha >\cong Z_4$, where

$$\alpha = (P_1, P_2, P_3, P_4)(P_5, P_6, P_7, P_8).$$

We conclude $|G| = 6 \cdot 4 = 24$. Similarly $G_{F_2} =< \beta >\cong Z_4$, where

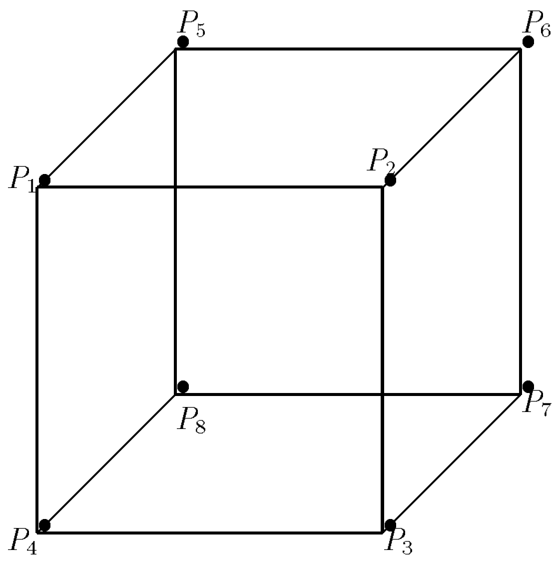
$$\beta = (P_1, P_5, P_8, P_4)(P_2, P_6, P_7, P_3).$$

Problem (3.1) (octahedral group) *Let G be the group of rotations fixing the unit cube. With the notation introduced above show the following:*

1. $G =< \alpha, \beta >$.
2. $G \cong S_4$.

For part 2. consider the action of G on the four pairs of opposite vertices: $A = \{P_1, P_7\}, B = \{P_2, P_8\}, C = \{P_3, P_5\}, D = \{P_4, P_6\}$.

It follows from Corollary (1.2) that the conjugacy classes of S_4 are in bijection with the partitions of the number 4. Aside of the neutral element we have eight elements of order 3, six elements of order 4, three involutions of cycle type (2,2) in the natural representation (forming the normal subgroup V together with the neutral element), and six involutions, which act as transpositions. We can see the operation of these elements on the cube: The elements of order 3 have as axis a line through two opposite vertices. They rotate by $2\pi/3$. The elements of order 4 and the three special involutions have as axis a line through the centers of two opposite faces. The remaining six involutions have as axis a line through the centers of two opposite edges. Rotation is by an angle of π.



Our main tool will be the cycle index:

Definition (3.1) (cycle index) *Let G be a finite group operating on the n-set Ω. For every $g \in G$ denote by $f_i = f_i(g)$ the number of cycles of g of length i. Observe $\sum_{i=1}^{n} f_i(g) = n$. The* **cycle index** *of (G, Ω) is defined as*

$$P_G(Z_1, Z_2, \ldots, Z_n) = \frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{n} Z_i^{f_i(g)}.$$

If $a_G(f_1, \ldots, f_n)$ denotes the number of elements of $g \in G$ satisfying $f_i(g) = f_i$, then we can write this equivalently as

$$P_G(Z_1, Z_2, \ldots, Z_n) = \frac{1}{|G|} \sum_{f_1, \ldots, F_n} a_G(f_1, \ldots, f_n) \prod_{i=1}^{n} Z_i^{f_i}.$$

We can now state and prove Pólya's main theorem. It is a little more general than what we have motivated above in the sense that instead of counting orbits of G in C^Ω we work with weights.

Definition (3.2) (weights) *Let G be a finite group operating on the n-set Ω, with the induced action on the set C^Ω of colorings.*
Let $R \supseteq \mathbb{Q}$ be a commutative ring, w a function $w : C \longrightarrow R$. We interpret

$w(c)$ as the **weight** *of colour c. Denote by $\mathcal{B}$ the set of orbits of G on the colorings. Let χ be a coloring. We define the weight of χ by*

$$w(\chi) = \prod_{x\in\Omega} w(x\chi).$$

As each $g \in G$ permutes the elements of Ω it is clear that w is constant on orbits. We can interpret w as a function $w : \mathcal{B} \longrightarrow R$.

Theorem (3.1) (Pólya's theorem) *Let G be a finite group operating on the n-set Ω, C a finite set (the colours). Consider the induced action of G on the set C^Ω of colorings.*
Let $R \supseteq \mathbb{R}$ be a commutative ring, $w : C \longrightarrow R$. Let w also be defined on C^Ω and on the set $\mathcal{B}$ of G-orbits on C^Ω, as in Definition (3.2). Then the following holds:

$$\sum_{B\in\mathcal{B}} w(B) = P_G(\sum_{c\in C} w(c), \sum_{c\in C} w(c)^2, \ldots).$$

Here P_G denotes the cycle index of G in its operation on Ω. In words: In order to obtain the sum of the weights of the orbits we have to evaluate the cycle index $P_G(Z_1, Z_2, \ldots, Z_n)$ at $Z_i = \sum_{c\in C} w(c)^2$.

Proof: We will see that all we need for the proof is the Burnside lemma (2.2). In fact, fix an orbit $B \in \mathcal{B}$ and apply the Burnside Lemma. We obtain

$$1 = \frac{1}{|G|} \sum_{g\in G} |F(g) \cap B|.$$

Here $F(g) \cap B$ is the set of colorings in the same orbit B, which are fixed under g. Multiply with $w(B)$:

$$w(B) = \frac{1}{|G|} \sum_{g\in G} \sum_{\chi\in B, \chi g=\chi} w(\chi).$$

Sum up over $\mathcal{B}$:

$$\sum_{B\in\mathcal{B}} w(B) = \frac{1}{|G|} \sum_{g\in G} \sum_{\chi\in F(g)} w(\chi).$$

Comparison with the definition of the cycle index shows that it suffices to prove the following:
For every $g \in G$ we have

$$\sum_{\chi \in F(g)} w(\chi) = \prod_{i=1}^{n} (\sum_{c \in C} w(c)^i)^{f_i}.$$

Here the $f_i = f_i(g)$ are as in Definition (3.1). If we realize that g has f_i cycles of length i and that a coloring χ is fixed by g if and only if it is constant on cycles we see that this is really a triviality.■

Let us use this Theorem to solve the two motivational problems: the discussion following Problem (3.1) shows that the cycle index of the octahedral group $G \cong S_4$ in its operation on the six faces of the cube is

$$P_G = \frac{1}{24}(Z_1^6 + 3Z_1^2 Z_2^2 + 6Z_1^2 Z_4 + 6Z_2^3 + 8Z_3^2). \tag{3.1}$$

As we wish to count orbits we should define the weight of each of the two colours to be 1. The number of orbits of colorings of the faces of the cube with 2 colours is therefore

$$P_G(2, 2, \ldots) = \frac{1}{24}(2^6 + 3 \cdot 16 + 6 \cdot 8 + 6 \cdot 8 + 8 \cdot 4) = 10.$$

Let us consider the second motivational Problem, the number of isomorphism classes of graphs on 5 vertices. We have listed the conjugacy classes of S_5 in its natural action on 5 points in the proof of Theorem (1.7). The operation on the 10 pairs is easily deduced from this. The corresponding cycle index (of the operation of S_5 on 10 objects) is

$$P_G = \frac{1}{120}(Z_1^{10} + 24Z_5^2 + 20Z_1Z_3^3 + 10Z_1^4Z_2^3 + 15Z_1^2Z_2^4 + 30Z_2Z_4^2 + 20Z_1Z_3Z_6). \tag{3.2}$$

As before we colour with two colours and wish to compute the number of orbits. We obtain the number of isomorphism classes of simple graphs on 5 vertices as

$$P_G(2, 2, \ldots) = 34.$$

Problem (3.2) *1. Determine the number of nonisomorphic graphs on 4 vertices.*

2. Determine the number of essentially different colorings of the faces of a die with m colours.

The **universal** way to use the weights in Pólya's theorem is to work with the polynomial ring $R = \mathbb{R}[x_c | c \in C]$ in $|C|$ variables and to define $w(c) = x_c$. All other choices of weights can be obtained by specialization. With the universal choice we get $w(f) = \prod_{c \in C} x_c^{n_c}$, where $n_c = f^{-1}(c)$. Let us apply the universal choice of weights to the operation of S_5 on the 10 points of $\binom{F}{2}$, whose cycle index has been given in equation 3.2. With weights $w(e) = x, w(n) = y$ the right side in Theorem (3.1) becomes

$$P_G(x+y, x^2+y^2, \ldots, x^6+y^6) = x^{10} + x^9y + 2x^8y^2 + 4x^7y^5 + 6x^6y^4 + \\ +6x^5y^5 + 6x^4y^6 + 4x^3y^7 + 2x^2y^8 + xy^9 + y^{10}$$

The coefficients tell us that there are precisely six nonisomorphic graphs with five edges and also 6 nonisomorphic graphs with six edges, for example. The sum of all coefficients is 34, the number of isomorphism classes of graphs on five vertices, as it has to be. We see that the universal choice of weights gives us more information than the earlier specific choice.

Problem (3.3) *Consider the operation of the octahedral group $G \cong S_4$ on the faces of a die. Determine the number of orbits of G on subsets of any fixed cardinality (between 1 and 6) of the set of faces.*

Chapter 4

Block designs

In this chapter we use permutation groups in the construction of an important class of combinatorial objects, block designs.

Definition (4.1) (**t-designs**) *Let Ω be a set of cardinality n and $\mathcal{B}$ a family of k-subsets of Ω. The pair $(\Omega, \mathcal{B})$ is a (**simple**) t-**design** if for every t-subset $T \subset \Omega$ there are exactly λ subsets $B \in \mathcal{B}$ such that $B \supseteq T$, for some natural number λ. The subsets $B \in \mathcal{B}$ are called the **blocks** of the design. More precisely the parameters of the design are then denoted as*

$$t - (n, k, \lambda).$$

There are many variants of this definition. We mention some of them, but as we will use mostly simple t-designs in the sequel we will not be very formal. If k-subsets are allowed to be counted more than once as a block we speak of a (not necessarily simple) $t-$design. t-designs with $\lambda = 1$ are also known as **Steiner systems.** In the case of Steiner systems we will also use the shorter notation $S(t, k, n)$ instead of $t - (n, k, 1)$. If we generalize the notion of a design in the sense that we use blocks not all of the same cardinality k one speaks of t-wise balanced designs. We obtain a trivial structure by choosing $\mathcal{B}$ to be the family of all k-subsets of Ω. This **complete design** has parameters $t - (n, k, \binom{n-t}{n-k})$. In order to exclude trivial cases we assume $t < k < n$. Consider pairs (T, B), where $|T| = t, B \in \mathcal{B}$ and $T \subset B$. Counting these pairs in two ways we arrive at the following equation:

$$\binom{n}{t} \cdot \lambda = b \cdot \binom{k}{t} \tag{4.1}$$

relating the parameters of a design $t-(n,k,\lambda)$. Here $b=|\mathcal{B}|$ denotes the number of blocks. Next we wish to show that a t-design is also $(t-1)$-design (if $t \geq 2$). It follows by induction that any t-design is an i-design for all $i \leq t$. If the value of t is in doubt we write λ_t instead of λ. The $\lambda-$parameter when the same design is considered as an i-design is then denoted by λ_i.

Lemma (4.1) *Let $\mathcal{D}$ be a design $t-(n,k,\lambda)$. Then $\mathcal{D}$ is also a $(t-1)$-design, where*

$$\lambda_{t-1} = \lambda \cdot (n-t+1)/(k-t+1).$$

Proof: Fix a $(t-1)$-subset $T' \subset \Omega$. The number of blocks containing T' is $\lambda_{t-1} = (n-t+1)\lambda/(k-t+1)$. Not clear yet? Count pairs (x,B), where $x \notin T', B \supset T' \cup \{x\}$. Counting in two ways we get $(n-t+1)\lambda = \lambda_{t-1}(k-t+1)$.■
By induction we arrive at the following formula for λ_i :

$$\lambda_i = \lambda \cdot \frac{\binom{n-i}{t-i}}{\binom{k-i}{t-i}} \tag{4.2}$$

We describe briefly some straightforward constructions.

Lemma (4.2) *Let $\mathcal{D} = (\Omega, \mathcal{B})$ be a simple design with parameters $t-(n,k,\lambda)$.*

1. *Choose as blocks all the k-sets which are not blocks of $\mathcal{D}$. Comparison with the complete design shows that this yields a design $t-(n,k,\binom{n-t}{n-k}-\lambda)$, the* **complementary design.**

2. *Fix a set I of i points, where $i<t$ and use as blocks the $B-I$, where B varies through the blocks of $\mathcal{D}$, which contain I. We obtain a design $(t-i)-(n-i,k-i,\lambda)$, a* **derived design.**

3. *Let the blocks of $\mathcal{D}'$, the* **supplementary design,** *be the complements of the blocks of $\mathcal{D}$. This yields a t-design with block-size $k'=n-k$. In order to determine its $\lambda-$value we can compare equation 4.1 with the corresponding expression for $\mathcal{D}'$. Observe that the number b of blocks is the same for both designs. By division we obtain the parameters of $\mathcal{D}'$ as*

$$t-(n,n-k,\lambda \cdot \frac{\binom{n-k}{t}}{\binom{k}{t}}).$$

4. *Fix a point P and choose as blocks of the* **residual design** $\mathcal{D}'$ *all the blocks of $\mathcal{D}$ avoiding P. It is clear that we obtain a $(t-1)$-design on $n-1$ points. In fact, the $\lambda-$value of $\mathcal{D}'$ is $\lambda' = \lambda_{t-1} - \lambda = \lambda \cdot (\frac{n-t+1}{k-t+1} - 1) = \lambda \cdot \frac{n-k}{k-t+1}$. We conclude that $\mathcal{D}'$ has parameters $(t-1)-(n-1, k, \lambda \cdot \frac{n-k}{k-t+1})$.*

Definition (4.2) *Let $\mathcal{D} = (\Omega, \mathcal{B})$ and $\mathcal{D}' = (\Omega', \mathcal{B}')$ be designs. An* **isomorphism** *from $\mathcal{D}$ to $\mathcal{D}'$ is a bijective mapping : $\Omega \longrightarrow \Omega'$, which induces a bijection between the blocks. An* **automorphism** *of $\mathcal{D}$ is an isomorphism from $\mathcal{D}$ to itself. The automorphism group $Aut(\mathcal{D})$ is the group of all automorphisms of $\mathcal{D}$. Observe that $Aut(\mathcal{D})$ is by definition a subgroup of the symmetric group on Ω.*

4.1 Some easy direct constructions

Let $E \cong E(2^n)$ be an elementary abelian group, equivalently the additive group of a vector space of dimension n over $\mathbb{F}_2$. We will in fact use additive notation. We define a 4-set $B = \{a, b, c, d\} \subset E$ to be a block if $a+b+c+d = 0$. This gives us a Steiner 3-design $S(3, 4, 2^n)$. In fact, let $T = \{a, b, c\}$ be a 3-set. There can be at most one block containing T, given by $d = a + b + c$. The only thing that could conceivably go wrong is that $d \in T$. In that case T would not be contained in a block at all. Assume without restriction $d = a$. We see that this cannot happen as it would follow $b = c$, contradiction. We have proved the following:

Theorem (4.1) *The 4-subsets of an elementary abelian 2-group, whose elements sum to zero, form the blocks of a Steiner 3-design*

$$S(3, 4, 2^n), \text{ for all } n \geq 4.$$

Next we define projective planes: Let $V = V(3, q)$ be a 3-dimensional vector space over the field $\mathbb{F}_q$. As points choose the $(q^3 - 1)/(q - 1) = q^2+q+1$ subspaces of dimension 1. As blocks (lines) choose the 2-dimensional subspaces, with the natural inclusion relation. We see that the number of lines equals the number of points: $b = n = q^2 + q + 1$. Each line has $(q^2 - 1)/(q-1)$ points, each point is on $q+1$ lines, any pair of points is on precisely one line and any two lines have precisely one point in common. In particular we have an $S(2, q + 1, q^2 + q + 1)$.

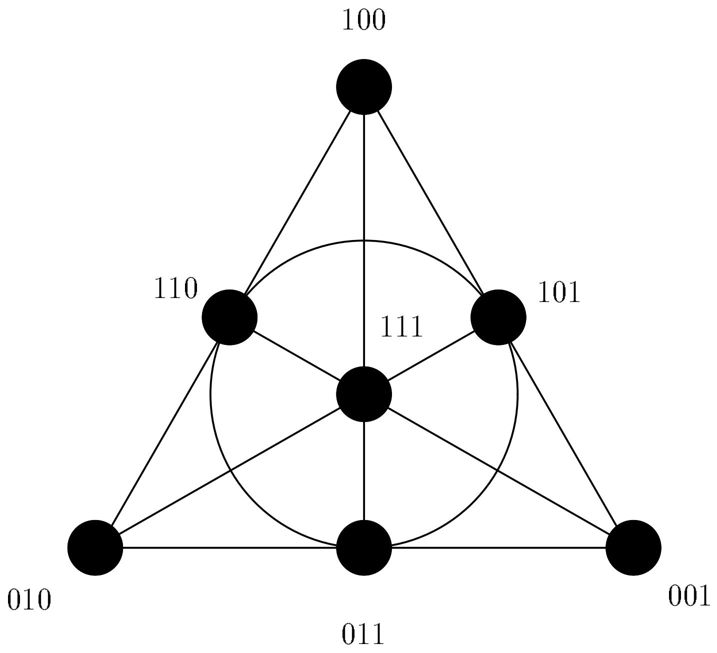
Definition (4.3) *Let q be a prime-power.*
The 1-dimensional and 2-dimensional subspaces of a 3-dimensional vector space over $\mathbb{F}_q$ form the points and lines (blocks) of the (classical) **projective plane** *of order q. This is a Steiner system $S(2, q+1, q^2+q+1)$. It has the property that any pair of lines intersects in precisely one point.*
Fix a line l, consider only the points off l (the **affine points***). The structure induced is a Steiner system $S(2, q, q^2)$ (the (classical)* **affine plane** *of order q.) In general $S(2, n+1, n^2+n+1)$ are called* **projective planes** *of order n and $S(2, n, n^2)$ are* **affine planes** *of order n.*

Problem (4.1)

1. *Show that every projective plane has the property that any two different lines have precisely one point in common.*
2. *Show that affine planes have the following property: If l is a line and P a point not on l, then there is precisely one line h through P, which intersects l trivially (is* **parallel** *to l).*
3. *Show that an affine plane of order n exists if and only if a projective plane of order n exists.*
4. *Show that the classical affine plane of order 3 as defined in Definition (4.3) is the only $S(2, 3, 9)$.*

It is an open problem if projective planes of nonprimepower orders exist.

Designs $S(2, 3, n)$ are also known as **Steiner triple systems,** $S(3, 4, n)$ are **Steiner quadruple systems.** We have seen that the projective plane of order 2 is a Steiner triple system $S(2, 3, 7)$. This design is uniquely determined by its parameters and is also known as the **Fano plane.**



The Fano plane

Symmetric designs are by definition 2-designs with equally many blocks as points. Symmetric designs with $\lambda = 2$ are also known as **biplanes.** Here is an easily constructed biplane:

Theorem (4.2) *Order 16 points in a square. Each point P defines a block B_P in the following way: the points of B_P consist all the points in the same row and all the points in the same column of P, but not P. This defines a design* $2 - (16, 6, 2)$.

4.2 Steiner triple systems

In this section we use a construction of Richard Wilson [11] to show that Steiner triple systems $S(2, 3, n)$ exist for all conceivable n. What are these conceivable n? Fix a point. As all remaining points occur in pairs n must be odd. Equation 4.1 yields $b = n(n-1)/6$. It follows that n must be 0 or 1 mod 3. We have seen that necessarily $n \equiv 1, 3 \pmod 6$.

Remains to shows that an $S(2,3,n)$ exists whenever this condition is satisfied. Put $m = n-2$. Then $m \equiv \pm 1 \pmod 6$, in words: m is odd and not divisible by 3. Let G be an abelian group of order m. Write G additively. Denote by Δ the family of triples $\{x,y,z\} \subset G - \{0\}$ satisfying $x+y+z=0$. Define a graph Γ with $G-\{0\}$ as set of vertices by joining x,y by and edge if $\{x,y\}$ is not contained in any triple from Δ. We will have to study the structure of this graph for a while.

Definition (4.4) *A* **1-factor** *of a graph is a collection of edges, which partition the vertices. A* **1-factorization** *of a graph is a partitioning of the edge set in 1-factors.*

Clearly 1-factors can only exist when the number of vertices is even.
It is obvious that the edges $\{x,-x\}$ form a 1-factor of Γ. Assume $\{x,y\}$ is an edge of Γ and $y \neq -x$. Then either $-(x+y) = x$ (and $y = -2x$) or $-(x+y) = y$ (and $y = -\frac{1}{2}x$). Observe that each vertex x really has three different neighbours (if $-\frac{1}{2}x = -2x$, then $3x = 0$, which is impossible as m is not divisible by 3). Graphs with valency 3 are also known as **cubic graphs.**

Lemma (4.3) *The graph* Γ *possesses a 1-factorization.*

Such a 1-factorization necessarily consists of three 1-factors. It suffices to prove that each connected component of Γ has a 1-factorization. Consider the graph Γ' at first, which arises out of Γ by omitting the edges $\{x,-x\}$. As Γ' is regular of degree two, it is a union of cycles. Consider the cycle C of Γ' containing vertex x. The vertices in C are $x, -2x, 4x, -8x, 16x, \ldots$. Observe that the mapping $x \mapsto -2x$ is an automorphism of the group G as G is abelian of odd order. We distinguish two cases:
Assume $-x \in C$. Then C has even length and for every $y \in C$ we have that $-y$ is opposite to y in C. In particular C is a connected component of Γ.
Assume $-x \notin C$. Then $-C$ has the same length as C and the connected component of Γ containing x is $C \cup (-C)$.
We can now prove the Lemma: in the first case the connected component is a cycle of even length, with opposite vertices joined. It is rather obvious how a 1-factorization can be constructed. In the second case the connected component is the union of two cycles of the same length, with corresponding vertices joined. A construction of a 1-factorization is a little trickier in this case, but not hard. We leave this as a problem

Problem (4.2) *Construct a 1-factorization for each of the following cubic graphs on $2u$ vertices:*

- *Vertices are elements of $\mathbb{Z}/2u\mathbb{Z}$, edges are the $\{i, i+1\}$ and the $\{i, i+u\}$.*
- *Vertices are the elements of $(\mathbb{Z}/u\mathbb{Z}) \times \{0,1\}$ with edges $\{(i,0),(i+1,0)\}, \{(i,1),(i+1,1)\}$ and $\{(i,0),(i,1)\}$.*

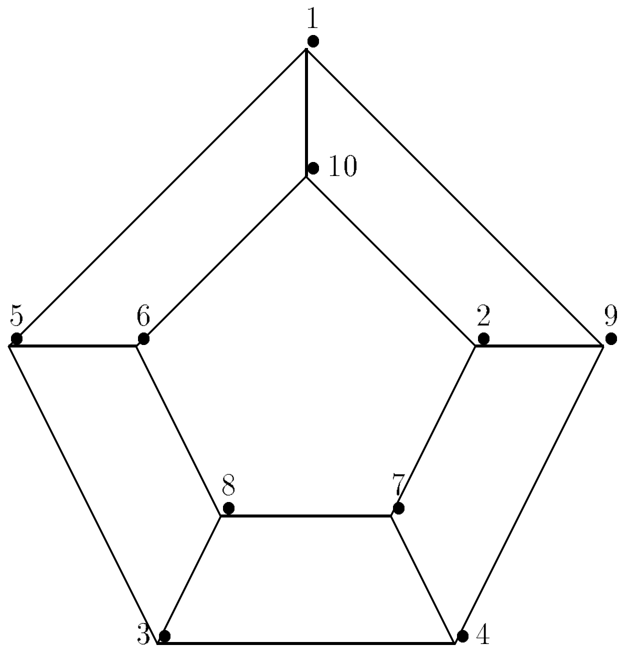
Let now F_1, F_2, F_3 the 1-factors of a 1-factorization of Γ. Let $\Omega = (G - \{0\}) \cup \{a_1, a_2, a_3\}$. We define the blocks of a Steiner triple system on Ω :
If x, y, z are different elements of $G - \{0\}$ such that $x + y + z = 0$, then $\{x, y, z\}$ is a block of type I.
If $\{x, y\}$ is an edge of Γ, then it belongs to one of our 1-factors, say F_i. Define $\{x, y, a_i\}$ to be a block (type II).
Finally, $\{a_1, a_2, a_3\}$ is the only block of type 0. It is now easy to check that we have constructed a Steiner triple system. We have proved the following:

Theorem (4.3) *A Steiner triple system $S(2,3,n)$ exists if and only if $n \equiv 1, 3 \pmod 6), n \geq 3$.*

We know $S(2,3,3)$ (trivial), $S(2,3,7)$ (the Fano plane) and $S(2,3,9)$ (the affine plane of order three). Let us carry through Wilson's construction to find an $S(2,3,13)$: The group is $G = \mathbb{Z}/11\mathbb{Z}$, the cyclic group of order 11. We have $\Omega = \{1,2,3,4,5,6,7,8,9,10,a_1,a_2,a_3\}$. The number of blocks is $b = n(n-1)/6 = 26$. Blocks of type I are the triples of nonzero residues mod 11 with vanishing sum. This gives us the complete list of blocks of types 0 and I:

a_1	a_2	a_3
1	2	8
1	3	7
1	4	6
2	3	6
2	4	5
3	9	10
4	8	10
5	7	10
5	8	9
6	7	9

Graph Γ looks as follows:



Here is a 1-factorization:

F_1 :	1,9	3,4	2,10	7,8	5,6
F_2 :	1,5	4,9	6,10	2,7	3,8
F_3	3,5	6,8	1,10	2,9	4,7

This gives us the fifteen remaining blocks:

a_1	1	9
a_1	3	4
a_1	2	10
a_1	7	8
a_1	5	6
a_2	1	5
a_2	4	9
a_2	6	10
a_2	2	7
a_2	3	8
a_3	3	5
a_3	6	8
a_3	1	10
a_3	2	9
a_3	4	7

4.3 Some easy recursive constructions

Theorem (4.4) (Moore) *If an $S(2, q, a)$ and an $S(2, q, b)$ exist, where q is a prime-power, then an $S(2, q, a \cdot b)$ exists.*

Proof: Arrange the points in an (a, b)-rectangle. Define the structure of an $S(2, q, a)$ on the set of rows (the row system) and the structure of an $S(2, q, b)$ on the set of columns (the column system). Moreover impose the structure of an $S(2, q, b)$ on each row and the structure of an $S(2, q, a)$ on each column. We use all these as blocks and call these blocks of type I. The remaining blocks will be of a different type: Consider the (q, q)-rectangles consisting of the points whose first coordinates form a block of the row system and whose last coordinates form a block of the column system. Impose the structure of an affine plane A of order q on these q^2 points in such a way that the rows and columns are blocks. Observe that this can be arranged. As blocks of type II we choose all the blocks of A aside of the rows and columns. It is now an elementary task to check that we obtain an $S(2, q, a \cdot b)$.■

As an illustration the reader should check how this construction, when applied to two copies of the trivial system $S(2, 3, 3)$ yields an $S(2, 3, 9)$, which latter is the affine plane of order 3 (see Problem (4.1)). In fact, we obtain the 9 points arranged in a square and the 12 lines are the following: the rows, the columns and the sets of three points whose first and second coordinates are different.

Theorem (4.5) (Skolem) *If an $S(2, q+1, n)$ exists, where q is a prime-power, then an $S(2, q+1, q \cdot n + 1)$ exists.*

Proof: Write the point set as $X \cup \{\infty\}$, where the $q \cdot n$ points in X are arranged in a rectangle. The blocks will be of three kinds:

- The union of a column and ∞ is a block (type I).
- Impose the structure of an $S(2, q+1, n)$ on each row. Use all these blocks (type II).
- Impose the structure of an $S(2, q+1, n)$ on the set of columns. Consider the $(q, q+1)$-rectangles R whose second coordinates form a block. Impose the structure of a projective plane of order q on each such set $R \cup \{\infty\}$ in such a way, that the unions of ∞ and the columns of R are lines. Take as blocks (type III) all the lines of these projective planes not passing through ∞.

■

Theorem (4.6) (Witt) *If $S(3, 4, a)$ and $S(3, 4, b)$ exist, then $S(3, 4, a \cdot b)$ can be constructed*

Proof: Write the point set as an (a, b)-rectangle. The blocks will be the following 4-subsets:

- Impose the structure of an $S(3, 4, b)$ on each row, proceed analogously for columns. Use all these sets as blocks (type I).
- Take all quadrangles as blocks. More precisely these are point sets of the form $\{(a_i, b_j) | i = 1, 2; j = 1, 2\}$ (type II).

- Take all points sets of the form $\{(a_1,b_1),(a_1,b_2),(a_2,b_3),(a_2,b_4)\}$, where the b_j are different (point sets on two different rows, two from each row, all from different columns). Do the analogous thing for columns. This yields the blocks of type III.

- Impose the structure of an $S(3,4,b)$ on the set of rows, analogously for the columns. Consider the $(4,4)$-rectangles A of points whose first and second coordinates form blocks of these row system and column system, respectively. Choose as blocks of type IV all 4-sets from such rectangles A with different row coordinates and different column coordinates.

■

Problem (4.3) *Use a variant of the construction in Theorem (4.6) to prove the following:*
If an $S(3,4,n)$ exists, then an $S(3,4,2n)$ exists.

4.4 A link to permutation groups

We describe a straightforward connection between permutation groups and block designs.

Definition (4.5) *A permutation group (G,Ω) is t-homogeneous if G is transitive in its operation on the unordered t-subsets of Ω.*

It is clear that t-transitive permutation groups are t-homogeneous (see Definition (2.2)).

Theorem (4.7) *Let the permutation group (G,Ω) be t-homogeneous, where $|\Omega|=n$. Choose a k-subset $B\subset\Omega$, where $t<k<n$. Let $\mathcal{B}=B^G$ be the orbit of B under the action of G. Then $(\Omega,\mathcal{B})$ is a t-design.*

This is in fact trivial. Let us calculate the $\lambda-$parameter. Equation 4.1 simplifies as we can calculate b. In fact, it follows from Lemma (1.9) that $b=|G|/|G_B|$. Here $G_B=\{g|g\in G, Bg=B\}$ is the **set-stabilizer** of B (see Definition (1.18)). It follows

$$\lambda=\frac{|G|\binom{k}{t}}{|G_B|\binom{n}{t}} \tag{4.3}$$

4.5 The groups $PGL_2(q)$

We have introduced the general linear groups in Example (1.3). In particular $GL_2(q)$ has order $(q^2-1)(q^2-q)$.

Problem (4.4) *Show that the center Z of $GL_2(q)$ consists of the scalar matrices and is therefore a cyclic group of order $q-1$.*

The factor group $PGL_2(q) = GL_2(q)/\mathbb{Z}(GL_2(q))$ is called the **projective general linear group**. It has order $(q+1)q(q-1)$. As the determinant is multiplicative we get a group homomorphism $det : GL_2(q) \longrightarrow \mathbb{F}_q^*$, which is of course onto. The kernel of det is known as $SL_2(q)$, the **special linear group.** We know that $SL_2(q) \lhd GL_2(q)$ and $GL_2(q)/SL_2(q) \cong Z_{q-1}$. In particular $SL_2(q)$ and $PGL_2(q)$ have the same order $(q+1)q(q-1)$. Clearly $Z \cap SL_2(q) \lhd SL_2(q)$. Put $d = |Z \cap SL_2(q)|$. A scalar matrix $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ belongs to $SL_2(q)$ if and only if $\lambda^2 = 1$. It follows that $d = 1$ if q is even whereas $d = 2$ if q is odd. We can also say that $Z \cap SL_2(q)$ is generated by the matrix $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, but in characteristic 2 we have $-1 = 1$. The factor group $PSL_2(q) = SL_2(q)/(Z \cap SL_2(q))$ is the **projective special linear group.** Its order is $(q+1)q(q-1)/d$. Consider the canonical mapping $\pi : SL_2(q) \longrightarrow PGL_2(q)$. The kernel of π is $Z \cap SL_2(q)$. It follows that π induces an injective mapping : $PSL_2(q) \longrightarrow PGL_2(q)$. We may see $PSL_2(q)$ as a normal subgroup of $PGL_2(q)$. Its index is d. In particular we have $PGL_2(q) = PSL_2(q)$ when q is a power of 2.
Clearly $GL_2(q)$ operates as a transitive permutation group on the q^2-1 nonzero vectors of the underlying vector space V. It also operates on the $(q^2-1)/(q-1) = q+1$ one-dimensional subspaces of V. However, the elements of Z (the scalar matrices) belong to the kernel of this permutation representation.

Problem (4.5) *Prove that the kernel of $GL_2(q)$ in its permutation representation on the $q+1$ one-dimensional subspaces of V is precisely the center Z.*

It follows that $PGL_2(q)$ operates as a permutation group on the set of one-dimensional subspaces of V. This set is known as the **projective line.**

Definition (4.6) *The projective line $\mathcal{P}_1(q)$ is the set of all one-dimensional subspaces of some two-dimensional vector space over the field $I\!F_q$.*

It is easier to calculate with the operation of $PGL_2(q)$ on the projective line when coordinates are introduced. So let $V = I\!F_q^2$. Represent the subspace generated by $(\tau, 1)$ as $\tau \in I\!F_q$ and the subspace generated by $(1, 0)$ by the symbol ∞. With this identification we can write

$$\mathcal{P}_1(q) = I\!F_q \cup \{\infty\}.$$

Let $g \in PGL_2(q)$ be represented by the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. We compute

$$(\tau, 1)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a\tau + c, b\tau + d).$$

It follows that $\tau g = \frac{a\tau+c}{b\tau+d}$ if $b\tau + d \neq 0$. If $b\tau + d = 0$, then $taug = \infty$. An analogous computation shows that $\infty g = \infty$ if and only if $b = 0$, and $\infty g = a/b$ otherwise. We conclude that the operation of $PGL_2(q)$ on the projective line is described as $\tau \longrightarrow \frac{a\tau+c}{b\tau+d}$ for $ad - bc \neq 0$. Here $\tau \in \mathcal{P}_1(q) = I\!F_q \cup \{\infty\}$ and the usual rules for calculation with ∞ have to be observed.

It is obvious that $G = PGL_2(q)$ is transitive on $\mathcal{P}_1(q)$. The stabilizer G_∞ consists precisely of the $q(q-1)$ mappings $\tau \longrightarrow a\tau + b$, where $a \neq 0$. If $x \in I\!F_q$ is given then $\tau \longrightarrow \tau + x$ affords the operation $0 \mapsto x$. We conclude that G is 2-transitive. The stabilizer $G_{(\infty,0)}$ consists of the mappings $\tau \longrightarrow a\tau$, where $a \in I\!F_q^*$. If $y \in I\!F_q^*$, then the unique element in $G_{(\infty,0)}$ affording the operation $1 \mapsto y$ is $\tau \longrightarrow y\tau$. We conclude that G is 3-transitive on the projective line.

Theorem (4.8) *The group $PGL_2(q)$ of order $(q+1)q(q-1)$ is 3-transitive in its operation on the projective line $\mathcal{P}_1(q)$. Given two order triples of different points from $\mathcal{P}_1(q)$ there is* **precisely one** *element $g \in PGL_2(q)$ mapping one triple onto the other ($PGL_2(q)$ is* **sharply** *3-transitive on the projective line).*

Problem (4.6) *Show that $PGL_2(q)$ is not 4-homogeneous on the projective line.*

4.5.1 Circle geometries

Next we construct a class of Steiner 3-designs on the projective line. We use Theorem (4.7) and in particular equation 4.3. So let $B \subset \mathcal{P}_1(q), |B| = k$. It follows from equation 4.3 that the design whose blocks are the images of B under $PGL_2(q)$ has parameters $3 - (q+1, k, \lambda)$, where $\lambda = k(k-1)(k-2)/|G_B|$. As λ cannot be smaller that 1 we obtain the following Corollary:

Corollary (4.1) *Let $B \subset \mathcal{P}_1(q), |B| = k$. Then the order of the set-stabilizer of B in $PGL_2(q)$ divides $k(k-1)(k-2)$.*

Let us work in $PGL_2(Q)$, where $Q = q^f$ and choose $B = \mathbb{F}_q \cup \{\infty\}$, in particular $k = q+1$. It is clear that $PGL_2(q) < PGL_2(Q)$ and that $PGL_2(q)$ stabilizes B. It follows from Corollary (4.1) that the set-stabilizer of B in $PGL_2(Q)$ must be $PGL_2(q)$. We obtain a 3-design on $Q+1$ with $\lambda = \frac{k(k-1)(k-2)}{(q+1)q(q-1)} = 1$.

Theorem (4.9) *Let $\Omega = \mathcal{P}_1(q^f)$. Choose as blocks the orbit containing $\mathbb{F}_q \cup \{\infty\}$ under the 3-transitive operation of $PGL_2(q^f)$. This yields a design*

$$3 - (q^f + 1, q + 1, 1) \text{ (a Steiner 3-design).}$$

In particular designs with these parameters exist for all prime-powers q and all natural numbers f.

Steiner 3-designs are also called **circle geometries,** for obvious reasons.

4.5.2 A class of 4-designs

We will use the groups $PGL_2(q)$ in characteristic two to construct families of 4-designs. As $PGL_2(q)$ is not 4-homogeneous on the projective line the simple method from Theorem (4.7) cannot be used. Our families will have block-sizes 5 and 6. We start by studying the operation of $PGL_2(q)$ a little more in detail.
So let $q = 2^f$ and assume that f is odd (equivalently $\mathbb{F}_4$ is not a subfield of $\mathbb{F}_q$). Put $G = PGL_2(q) = PSL_2(q)$. The sharp triple transitivity of G gives a lot of information on the operation of G. An immediate consequence is that the stabilizer of a 3-subset is precisely S_3.

Problem (4.7) *Let $S = \{\infty, 0, 1\}$. Describe all the elements of the stabilizer $PGL_2(q)_S$.*

We collect some more information:

Lemma (4.4) *Let $q = 2^f, G = PGL_2(q)$ in its operation of the projective line. Then the following hold:*

1. *An element $1 \neq g \in G$ has at most two fixed points.*
2. *Sylow-2-subgroups are elementary abelian*

Proof: It follows from sharp triple transitivity that an element with three fixed points is the identity. A Sylow-2-subgroup is given by the elements $\tau \longrightarrow \tau + x$, where $x \in \mathbb{F}_q$. This is clearly elementary abelian.■

Lemma (4.5) *Let $q = 2^f, f$ odd, and $G = PGL_2(q)$ in its operation of the projective line. Then the following hold:*

1. *Involutions have precisely one fixed point.*
2. *Elements of order 3 are fixed-point-free.*
3. *$|G|$ is not divisible by 5.*

Proof: Involutions certainly have at least one fixed point. If more, then they would have at least three fixed points, contradiction. As f is odd we have that $q+1$ is a multiple of three. As elements of order three cannot have three fixed points, they must be fixed-point-free. As f is odd we have that q is $\pm 2 \pmod 5$. It follows $(q+1)q(q-1)$ is not divisible by five.■

Let $S \subset \mathcal{P}_1(q)$ be a 4-subset. It follows from Corollary (4.1) that $|G_S|$ divides $8 \cdot 3$. An element of order 3 operating on a 4-set would have a fixed point. This cannot be the case. Moreover it is impossible that $|G_S| = 8$ as G_S would then have to be isomorphic to a Sylow-2-subgroup of S_4, which is a non-abelian group. We conclude that $|G_S|$ divides 4. In order to show equality it suffices to find a subgroup of order 4 of the stabilizer of S. To that end we can replace S by another 4-set from the same orbit. Because of the triple transitivity we can choose $S = \{\infty, 0, 1, a\}$ for some $a \in \mathbb{F}_q - \mathbb{F}_2$. The element $\tau \longrightarrow a/\tau$ and $\tau \longrightarrow (\tau + a)/(\tau + 1)$ are involutions. They commute and stabilize S.

Lemma (4.6) *Let $q = 2^f, f$ odd, and $G = PGL_2(q)$ in its operation of the projective line. Then the set-stabilizer G_S of a 4-set S is an elementary abelian group of order 4, with precisely one fixed point.*

In fact, G_S must have at least one fixed point, and cannot have three fixed points.
Let $F \subset \mathcal{P}_1(q)$ be a 5-subset. As $|G|$ is not divisible by 5 and elements of order 3 are fixed-point-free we conclude from Corollary (4.1) that $|G(F)|$ divides 4. It is clear that only two cases can occur: either G_F is trivial or G_F is a four-group.

Lemma (4.7) *Let $q = 2^f, f$ odd, and $G = PGL_2(q)$ in its operation of the projective line. Then the set-stabilizer G_F of a 5-set F is either trivial or an elementary abelian group of order 4, with precisely one fixed point.*

Define a design $\mathcal{D}$ on $\mathcal{P}_1(q)$ with block set $\mathcal{B}$ consisting of the 5-sets with a nontrivial stabilizer. As each such 5-set can be written in a unique way as the union of a 4-set S and the fixed point of G_S we see that the number of blocks is $b = \binom{q+1}{4}$. We claim that the parameters are $4-(q+1, 5, 5)$. Indeed, let $S = \{a, b, c, d\}$ be given. We have to count the elements $x \in \mathcal{P}_1(q) - S$ such that the 5-set $F = S \cup \{x\}$ has a nontrivial stabilizer. This stabilizer is then a four-group V. We see that the fixed point of V must be an element of F. If the fixed point is x, then $V = G_S$ and x is the fixed point of V. So assume the fixed point of V is in S. As G_S is transitive on S we may assume a is this fixed point. Then V must contain an element σ achieving the following operation: $\sigma(a) = a, \sigma : b \longleftrightarrow c, d \longleftrightarrow x$. Because of the sharp triple transitivity of G we see that an involution σ is uniquely determined by the first three operations. This shows that x is uniquely determined as image of d under σ. We see that the number of blocks containing S is indeed $\lambda = 1 + 4 \cdot 1 = 5$. We have proved the following:

Theorem (4.10) (Alltop's designs) *Let $q = 2^f, f$ odd, and $G = PGL_2(q)$ in its operation of the projective line. Let a 5-set $F \subset \mathcal{P}_1(q)$ be a block if and only if its stabilizer in G is nontrivial. This defines a simple design with parameters*

$$4-(2^f+1, 5, 5) \text{ for } f \text{ odd.}$$

4.6 The small Witt design

In section 2.2 we constructed the simple Mathieu group $G = M_{12}$ of order $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ in its sharply 5-transitive action on 12 points. We wish to use Theorem (4.7) to construct a 5-design with $k = 6$ on 12 points. We use the notation and results of section 2.2. Put $\Omega = \{E, T, 0, 1, \ldots, 9\}$. Blocks are defined in the following way: Let I be the conjugacy class of involutions having four fixed points. As the pointwise stabilizer of 4 points is a quaternion group of order 8 and as Q_8 has precisely one involution we see that $|I| = \binom{12}{4}$. Each $g \in I$ yields four blocks: the unions of the four fixed points of g and two more points in the same transposition of g. So, if $g = (a)(b)(c)(d)(e,f)(g,h)(i,j)(k,l)$, then $\{a,b,c,d,e,f\}$ and $\{a,b,c,d,g,h\}\ldots$ are blocks. How many blocks does this define and what is the stabilizer of a block?

We claim that each block is described precisely $\binom{6}{4} = 15$ times in this way. Concretely this claim says that if the involution g_1 fixing c,d,e,f has (a,b) as a transposition, then necessarily for every pair $\{x,y\} \subset B = \{a,b,c,d,e,f\}$ the involution g_2 with $B - \{x,y\}$ as set of fixed points maps $x \longleftrightarrow y$. As the symmetric groups are generated by transpositions this is equivalent with the statement that the set stabilizer of a block is as big as possible: $G_B \cong S_6$. As $(c,d) = (a,c)^{(a,d)}$ it suffices to show that all operations of type $(a,c)(b)(d)(e)(f)$ are induced by involutions in G. So let τ be the involution with b,d,e,f as fixed points. We have to show that the $a\tau = c$. Observe that all this happens in the stabilizer of three points (d,e,f). We see that we can work in the group $(M_{10})_0$ of order $9 \cdot 8$. We have seen that $(M_{10})_0$ is the semidirect product of the normal subgroup $E =< \phi_1, \phi_2 >\cong E(9)$ and the quaternion group $Q =< \theta, \lambda >$. Moreover Q is the stabilizer of a point. As $(M_{10})_0$ is sharply 2-transitive, stabilizers of different points intersect only in the identity. This shows that there are $9 \cdot 7 = 63$ nonidentity elements fixing one point each. Thus E consists of the identity and the eight fixed-point-free elements. These are of order three. Let $\sigma \in (M_{10})_0$ be the involution fixing a and let σ afford the operation $(a)(b,c)$. Let $\tau \in (M_{10})_0$ be the involution fixing b. We have to show that τ affords the operation $(b)(a,c)$. Assume this is not the case, so that τ maps $\tau = (b)(a,d)\ldots$. Choose e such that $\sigma = (a)(b,c)(d,e)\ldots$ As the factor group $(M_{10})_0/E$ has only one involution we conclude that $\sigma\tau \in E$. It follows that $\sigma\tau$ is fixed-point-free of order three. As $\sigma\tau$ affords the operation $e \mapsto a \mapsto d$ it follows that $d \mapsto e$. This shows

that *tau* must fix e. This is impossible as τ has only one fixed point.
We have proved our claim. It follows that for any block B the length of its orbit under the action of M_{12} is $|M_{12}|/6! = 132$. The total number of blocks is $\binom{12}{4} \cdot 4/15 = 132$. We conclude that M_{12} is transitive on the blocks. It follows from Theorem (4.7) that this defines a 5-design with $\lambda = 1$. We have seen the following:

Theorem (4.10) (small Witt design) *Consider the sharply 5-transitive action of M_{12} on the 12-set Ω. Define a 6-set B to be a block if there is an involution in M_{12}, which stabilizes B as a set and has four fixed points in B. There are 132 blocks. The set-stabilizer is $(M_{12})_B \cong S_6$. Further M_{12} is transitive on the blocks and these blocks define a Steiner 5-design*

$$S(5, 6, 12).$$

4.7 The projective linear groups

The linear groups $GL_n(q)$ had been introduced as Example (1.3). In section 4.5 we studied the projective linear groups in dimension $n = 2$. In this section we collect some facts about the structure of these groups in the general case. The more elementary facts are very similar to the 2-dimensional case:
The group $G = GL_n(q)$ has order $|GL(n, q)| = q^{n(n-1)/2} \prod_{i=1}^{n}(q^i - 1)$, as pointed out in Example (1.3). The center $Z = \mathbb{Z}(G)$ consists of the scalar matrices and is therefore cyclic of order $q - 1$. The factor group $GL_n(q)/Z = PGL_n(q)$ is the **projective general linear group.** The **special linear group** $SL_n(q)$ concists of the matrices with determinant 1. As kernel of the determinant we have $SL_n(q) \lhd GL_n(q)$, of index $q - 1$. In particular $SL_n(q)$ and $PGL_n(q)$ have the same order. The intersection $Z \cap SL_n(q)$ is a cyclic group and a normal subgroup of $SL_n(q)$. It consists of all scalar matrices $diag(\lambda)$, where $\lambda \in \mathbb{F}_q$ and $\lambda^n = 1$. It follows that $|Z \cap SL_n(q)| = gcd(n, q-1)$.
The **projective special linear group** is defined as the factor group

$$PSL_n(q) = SL_n(q)/(Z \cap SL_n(q).$$

We also see that $PSL_n(q) \trianglelefteq PGL_n(q)$.
The natural geometrical object on which $PGL_n(q)$ operates is the projective

$(n-1)$-dimensional geometry $\mathcal{P}_{n-1}(q)$. We have introduced the special case of the projective line $\mathcal{P}_1(q)$ in Definition (4.6).

Definition (4.7) (projective space) *Let $V = V(n,q)$ be an n-dimensional vector space over $\mathbb{F}_q$. The projective $(n-1)$-dimensional geometry $\mathcal{P}_{n-1}(q)$ has as objects the subspaces of dimensions between 1 and $n-1$. Here 1-dimensional subspaces are called* **points**, *2-dimensional subspaces are* **lines**, *and so on. The $(n-1)$-dimensional subspaces are* **hyperplanes.** *Incidence between objects is defined by inclusion. As Z fixes every subspace, we have a natural operation of $PGL_n(q)$ on the objects of $\mathcal{P}_{n-1}(q)$.*

Observe that the operation of $PGL_n(q)$ preserves incidence If for instance P is a point, l is a line and $\sigma \in PGL_n(q)$, then $P \in L$ if and only if $p\sigma \in l\sigma$.

Lemma (4.8) *$PSL_n(q)$ is 2-transitive on the points of $\mathcal{P}_{n-1}(q)$.*

Proof: It is easier to consider the operation of $SL_n(q)$. Let P_1, P_2 be two different points. Adapting the basis we see that the stabilizer of P_1 and P_2 in $SL_n(q)$ consists precisely of the matrices $\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \mu & 0 \\ * & * & A \end{pmatrix}$, where $\lambda, \mu \in \mathbb{F}_q^*$, $*$ denote arbitrary matrices and A is an $(n-2, n-2)$-matrix of determinant $\frac{1}{\lambda\mu.}$ It follows that the order of the stabilizer is $(q-1)^2 q^{2(n-2)} |SL_{n-2}(q) = \frac{q(q^n-1)(q^{n-1}-1)}{(q-1)^2}$. As this is the same as the number $\frac{q^n-1}{q-1}(\frac{q^n-1}{q-1} - 1)$ of pairs of points, we are done.■

Theorem (4.11) *$PGL_n(q)$ operates regularly on the ordered sets of $n+1$ points* **in general position** *of $\mathcal{P}_{n-1}(q)$. Here a set of points is in general position if any n of them generate the whole space.*

Proof: Sets of n points in general position correspond to a basis of the underlying vector space. It is clear that $PGL_n(q)$ permutes these transitively. So let $\{v_1, v_2, \ldots, v_n\}$ be a basis of $V = V(n,q)$. The stabilizer of the corresponding points $P_i = \mathbb{F}_q v_i$ in $GL_n(q)$ consists precisely of the diagonal matrices. A point $P = \mathbb{F}_q v$ complements the P_i to a set of points in general position if and only $v = \sum_{i=1}^n \lambda_i v_i$, where $\lambda_i \neq 0$ for all i. It is obvious that the scalar matrices are transitive on these vectors. The number of such $(n+1)-$tuples is

$$\frac{q^n-1}{q-1}\cdot\frac{q^n-q}{q-1}\cdot\ldots\cdot\frac{q^n-q^{n-1}}{q-1}\cdot\frac{(q-1)^n}{q-1}=|PGL_n(q)|.$$

■

4.8 The simplicity of $PSL_n(q)$.

Definition (4.8) (transvections) *An element $\tau\in SL_n(q)$ is called a* **transvection** *if one of the following equivalent conditions is satisfied:*

1. *$rank(\tau-I)=1$ and τ operates trivially on the image of $\tau-I$, (here I denotes the unit matrix).*
2. *There is a basis of V such that τ is represented by the matrix $\begin{pmatrix} I & 0\\ C & 1\end{pmatrix}$, where I is the $(n-1,n-1)$ unit matrix, 0 is a 0-column, C is an arbitrary nonzero $(1,n-1)-$ row and 1 is 1.*
3. *There is a hyperplane $H\subset V$, a vector $0\neq d\in H$ and a nonzero linear functional $\chi: V\longrightarrow \mathbb{F}_q$ with kernel H such that $v\tau=v+(v\chi)d$. We write then $\tau=\tau_{u,d}$ (and d is the* **direction** *of τ).*

The matrix representation shows that the transvections with respect to the same hyperplane H form a subgroup, that this subgroup is abelian and that every transvections has order p, where p is the prime a power of which is q.

Theorem (4.12) *The transvections form a conjugacy class of elements of order p in $GL_n(q)$.*

Proof: We know that each transvection has order p. As $GL_n(q)$ is transitive on hyperplanes it suffices to show that the transvections belonging to a fixed hyperplane H are conjugate. This is shown by the following calculation:

$$\begin{pmatrix} G^{-1} & 0\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix} I & 0\\ C & 1\end{pmatrix}\cdot\begin{pmatrix} G & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix} I & 0\\ CG & 1\end{pmatrix}.$$

■

Theorem (4.13) *Let $0 \neq d \in V = V(n,q)$. Let $T(d)$ consist of all transvections with direction d and the neutral element. Then $T(d)$ is a normal subgroup of the stabilizer of d in $GL_n(q)$. The group $T(d)$ is elementary abelian of order q^{n-1} and the stabilizer $GL_n(q)$ is a semidirect product of $T(d)$ and a group $GL_{n-1}(q)$.*

Proof: As $d \in H$ we have that every transvection with direction d fixes d. Let $\tau_i = \tau_{u_i,d}$, where $\tau_i : V \longrightarrow \mathbb{F}_q$ is a linear functional with kernel H_i and $d \in H_i$. We have $v\tau_1\tau_2 = (v + u_1(v)d)\tau_2 = v + u_1(v)d + u_2(v + u_1(d))d = v + (u_1(v) + u_2(v))d$. We see that $T(d)$ is an elementary abelian group. As there are precisely q^{n-1} functionals $: V \longrightarrow \mathbb{F}_q$ with d in their kernel we also obtain the order of $T(d)$.
Choosing d as first element of a basis we see that the stabilizer $GL_n(q)_d$ consists of the matrices of the form $\begin{pmatrix} 1 & 0 \\ C & A \end{pmatrix}$, where $A \in GL_{n-1}(q)$ and C is arbitrary. We can write $GL_n(q)_d$ as a semidirect product of $T(d)$ and of the complement consisting of the $\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}$.■

Theorem (4.14) *If either $n \geq 3$ or the characteristic is 2, then the transvections form a conjugacy class in $SL_n(q)$.*

Proof: We know that the transvections are contained in $SL_n(q)$ and that they form a conjugacy class in $GL_n(q)$. Fix a transvection τ As the index of $SL_n(q)$ in $GL_n(q)$ is $q-1$ we have to show that under the conditions above for every $\alpha \in \mathbb{F}_q^*$ there is an element of $GL_n(q)$ commuting with τ, whose determinant is α. In fact, choose $\begin{pmatrix} I & 0 \\ C & 1 \end{pmatrix}$, where $C = (1, 0, 0, \ldots, 0)$. Put $\rho = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & \lambda \end{pmatrix}$, where $\lambda \in \mathbb{F}_q^*$ and A is a regular $(n-2, n-2)-$matrix. Then $\rho\tau = \tau\rho$. If $n \geq 3$, then $det(A)$ attains any given value in $\mathbb{F}_q^*$. If $n = 2$, then λ^2 varies over all elements of $\mathbb{F}_q^*$, in characteristic 2.■

Problem (4.8) *Show that $SL_2(q)$ is generated by transvections.*

Theorem (4.15) *The transvections generate $SL_n(q)$.*

Proof: Let T be the set of transvections, $N =< T >$ the subgroup of $SL_n(q)$ generated by the transvections. Then $1 \neq N \trianglelefteq SL_n(q)$. We have to show that $N = SL_n(q)$. As $SL_n(q)$ is 2-transitive on the nonzero vectors (this follows from Lemma (4.8)) we conclude from Theorem (2.3) that N is transitive on the nonzero vectors. Let d be a nonzero vector. It suffices to show that N contains the stabilizer $SL_n(q)_d$. As $SL_n(q)_d$ is a semidirect product of $T(d)$ and the group consisting of the matrices of the form $\begin{pmatrix} 1 & 0 \\ C & A \end{pmatrix}$, where $A \in SL_{n-1}(q)$, we are in an inductive situation, the basis $n = 2$ being furnished by the preceding Problem. We can assume that $n \geq 3$ and that $SL_{n-1}(q)$ is generated by transvections. It is clear that these yield transvections of our complement. We have shown that $SL_n(q)_d$ is generated by transvections and are done.■

Lemma (4.9) *We have $SL_n(q)' = SL_n(q)$, unless $(n, q) = (2, 2)$ or $(n, q) = (2, 3)$.*

Proof: Because of the preceding Theorem (4.15) it suffices to show that each transvection is a commutator.
Let $n \geq 3, \tau \in T(d)$. From the description of $T(d)$ and $SL_n(q)_d$ we see that we can choose $\sigma \in T(d)$ and $g \in SL_n(q)_d$ such that $\sigma^g = \tau\sigma$. It follows $\tau = [\sigma, g]$.
In case $n = 2$ we calculate the following commutator in $SL_2(q)$:

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix} \cdot \begin{pmatrix} 1 & -\beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \beta(\alpha^2 - 1) \\ 0 & 1 \end{pmatrix}.$$

We have represented a transvection as a commutator in $SL_2(q)$ if we can find $\alpha \neq 0$ such that $\alpha^2 \neq 1$. This is always possible, with the exceptions of $q = 2$ and $q = 3$.■

Theorem (4.16) *$PSL_n(q)$ is a simple group, unless $(n, q) = (2, 2)$ or $(n, q) = (2, 3)$.*

Proof: Assume N is a nontrivial normal subgroup of $G = PSL_n(q)$. It follows from Theorem (2.3) that N is transitive on the points of $\mathcal{P}_{n-1}(q)$. Let $0 \neq d \in V$, put $P = \mathbb{F}_q d$. As the stabilizer of d in $GL_n(q)$ is a semidirect product with $T(d)$ as normal subgroup we conclude that $G_P = TH$, where $T \lhd G_P$ is the image of $T(d)$ mod Z (precisely $T = T(d)Z/Z$). In particular T is abelian. Consider the subgroup TN of G (see Lemma (1.6)). As it contains T and N is transitive on the points of $\mathcal{P}_{n-1}(q)$, we see that NT contains the images mod Z of all transvections. As the transvections generate $SL_n(q)$ we conclude $G = TN$. By the second isomorphism theorem (Theorem (1.2)) $G/N \cong T/(T \cap N)$. As T is abelian, G/N is abelian. Assume now we are not in one of the two exceptional situations. We have proved in Lemma (4.9) that $G = G'$. This means that G does not have any nontrivial abelian factorgroup (see Lemma (1.7)). We conclude $G = N$.$\blacksquare$

Problem (4.9) *Determine the structure of the groups $GL_2(2)$ and $GL_2(3)$. Show in particular that they are solvable.*

4.9 Quadrics and ovals

Projective geometries are important mainly because roots of homogeneous polynomials live in them. We illustrate this point by using the quadratic polynomial $Y^2 - XZ$ in three variables, whose coefficients we consider as elements of $\mathbb{F}_q$. If (x, y, z) is a solution vector, then also every scalar multiple $(\mu x, \mu y, \mu y)$ is, where $0 \neq \mu \in \mathbb{F}_q$. We can therefore view the set of roots to consist of points of $\mathcal{P}_2(q)$. This works for every homogeneous polynomial $p(X, Y, Z)$. Denote the set of its roots in $\mathcal{P}_2(q)$ by $V(p(X, Y, Z))$. Here the letter V stands for "variety". In general a **quadric** is the set of roots of a quadratic homogeneous polynomial. If the polynomial has n variables, then the quadric is a point set in the $(n-1)$-dimensional projective geometry.
It is easy to check that $V(Y^2 - XZ)$ consists of $q+1$ points, more precisely $V(Z^2 - XY) = \{(0:0:1)\} \cup \{P_\alpha | \alpha \in \mathbb{F}_q\}$, where $P_\alpha = (1 : \alpha : \alpha^2)$. We claim that no line contains more than two points of $V(Z^2 - XY)$. Equivalently we have to prove the following: if we write the vectors generating the points of $V(Z^2 - XY)$ as columns of a $(3, q+1)-$matrix, then any three columns are linearly independent. Such sets of three columns are of one of the following

two types, either $\begin{pmatrix} 0 & 1 & 1 \\ 0 & \alpha & \beta \\ 1 & \alpha^2 & \beta^2 \end{pmatrix}$ or $\begin{pmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{pmatrix}$. We leave it to the reader to check that these matrices have nonzero determinant.

Lemma (4.10) *Let X be a point set in $\mathcal{P}_2(q)$ such that no line contains more than two points of X. Then $|X| \leq q+2$.*

Proof: This follows from the fact that there are precisely $q+1$ lines through each point.■

Definition (4.9) ((hyper)ovals) *Let X be a point set in $\mathcal{P}_2(q)$ such that no line contains more than two points of X. If $|X| = q+1$, then X is an* **oval.** *If $|X| = q+2$, then X is a* **hyperoval.**

Theorem (4.17) *$\mathcal{P}_2(q)$ contains ovals.*

Proof: We have seen that $V(Y^2 - XZ)$ is an oval.■

Lemma (4.11) *If q is odd, then there are no hyperovals in $\mathcal{P}_2(q)$. If q is even, then every oval is embedded in a unique hyperoval.*

Proof: Let X be a hyperoval, P a point not in X. The points of X occur in pairs on lines through P. This shows that $q+2$. must be even. It follows that q is even.
Let new q be even, X an oval. We observe that every point of X is on precisely one tangent to X, the remaining q linea through the point passing through two points of X. As $q+1$ is odd we see that every point not in X is on at least one tangent to X. Let $N \notin X$ be a point, where two tangents to X intersect. Assume N is on a secant to X. Then N must also be on a line h missing X. As each point $\neq N$ on h is on some tangent, we see that the number of tangents is $> q+1$, contradiction. We conclude that all tangents intersect in the same point N (the **nucleus** of X), and $X \cup \{N\}$ is the unique hyperoval containing X.■

4.10 The large Witt designs

Our main aim in this chapter in the construction of a design $S(5,8,24)$, the **large Witt design.** If we fix three points of a hypothetical $S(5,8,24)$ and consider the blocks containing these three points we obtain a design $S(2,5,21)$ on the remaining points (see Lemma (4.2)). These are the parameters of a projective plane of order 4. We have seen in Definition (4.3) that the 2-dimensional projective geometry $\mathcal{P}_2(4)$ is an $S(2,5,21)$. We leave it as a (relatively difficult) problem to show that this is the only $S(2,5,21)$.

Problem (4.10) *Show that there is up to isomorphism only one $S(2,5,21)$ (= projective plane of order 4).*

Let Π be the point set of $\mathcal{P}_2(4)$. We use $\Omega = \Pi \cup \{a_1, a_2, a_3\}$ as set of points of the $S(5,8,24)$. We can use the sets $l \cup \{a_1, a_2, a_3\}$, where l runs through the 21 lines of $\mathcal{P}_2(4)$, as the family of blocks containing $\{a_1, a_2, a_3\}$. In order to be able and construct our design while also proving its uniqueness we need to know more about substructures of $\mathcal{P}_2(4)$ and the operation of $G = PGL_3(4)$ and $G_0 = PSL_3(4)$.

Problem (4.11) *Show that there is up to isomorphism only one $S(2,3,7)$ and that its full automorphism group is the simple group $GL_3(2) = PGL_3(2) = PSL_3(2)$ of order 168.*

We collect a few basic data: G_0 is a simple group of order $2^6 \cdot 9 \cdot 5 \cdot 7$ and a normal subgroup of index 3 in G. Clearly $\mathcal{P}_2(4)$ contains Fano planes (just consider the points corresponding to vectors all of whose entries are in the subfield $\mathbb{F}_2$). Each Fano plane is generated by each of its quadrangles (sets of four points in general position). Here we say that a point set X generates a projective subplane A if A is the smallest projective plane containing X. As G is transitive on quadrangles we conclude that G is transitive on the set of Fano planes contained in $\mathcal{P}_2(4)$. Clearly the stabilizer of a Fano plane in G is $GL_3(2)$. We conclude from the orbit length lemma that the number of Fano subplanes of $\mathcal{P}_2(4)$ is $|G|/168 = 360$. As $GL_3(2)$ is a simple group we see that it is contained in G_0. It follows again from the orbit length lemma that G_0 has three orbits of Fano planes, each of length 120.
We know that the number of (unordered) quadrangles is $|G|/4! = 7 \cdot 360$. The stabilizer of a quadrangle is S_4. As this group is generated by involutions,

we conclude that the stabilizer of a quadrangle is contained in G_0. It follows that G_0 has three orbits of quadrangles, each of size $7 \cdot 120$.

Lemma (4.12) *Each quadrangle of $\mathcal{P}_2(4)$ is contained in precisely one hyperoval. There are 168 hyperovals in $\mathcal{P}_2(4)$. The group G is transitive on hyperovals, while G_0 has three orbits of hyperovals, each of length 56.*

Proof: The first statement is best read off from a picture of the Fano plane. Let Q be a quadrangle and E the Fano plane containing Q. There is precisely one line in the Fano plane avoiding Q. This line has five points, three in E and two outside E. These two points are the only ones that complement Q to a hyperoval. We conclude that G is transitive on hyperovals. As there are $7 \cdot 360$ quadrangles, and each hyperoval contains 15 quadrangles, we count $7 \cdot 360/15 = 168$ hyperovals. The order of the stabilizer of a hyperoval in G is therefore $|G|/168 = 6!/2$. As this stabilizer is a subgroup of S_6 and A_6 is a simple group we conclude that the stabilizer of a hyperoval is A_6. By a by now familiar argument we conclude from the simplicity of A_6 that G_0 has three orbits on hyperovals.■

Lemma (4.13) *Each triangle in $\mathcal{P}_2$ is in precisely three hyperovals, one from each G_0-orbit.*

Proof: It is clear that G_0 is transitive on triangles. The rest follows from a familiar counting argument.■

We note that this suffices to construct $S(3,6,22)$: take as point set $\Pi \cup \{\infty\}$ and as blocks the lines of $\mathcal{P}_2(4)$, including ∞, as well as the hyperovals from one G_0-orbit. As we aim higher we have to work a little more.

Lemma (4.14) *The* **block intersection numbers** *of a design are the cardinalities of the intersections of two different blocks. For the designs involved here the possible block intersection numbers are:*

design	*block intersection numbers*
$S(2,5,21)$	*1*
$S(3,6,22)$	*0,2*
$S(4,7,23)$	*1,3*
$S(5,8,24)$	*0,2,4*

Proof: $S(2,5,21)$ is a projective plane. It follows that one two blocks intersect in one point. The statement on $S(3,6,22)$ follows. Proceeding like this we see that the only thing that remains to be proved is that block intersection number 0 cannot occur in $S(4,7,23)$. This follows from the usual counting arguments: in fact, fix a block B. As $\lambda_3 = 5$, we see that each of the 35 triples in B is contained in four blocks $\neq B$. It follows that $35 \cdot 4 = 140$ points intersect B in three points. Fix $P \in B$. As $\lambda_1 = 77$ and P is on 15 triples contained in B, we see that $77 - 1 - 15 \cdot 4 = 16$ blocks intersect B precisely in P. It follows that $16 \cdot 7 = 112$ blocks intersect B in cardinality 1. As $1 + 140 + 112 = 253$ happens to be the number of blocks of the design, we have proved that no two blocks intersect trivially.■

Lemma (4.15) *Let B be a block of our putative design $S(5,8,24)$. Put $A = \{a_1, a_2, a_3\}$. Then the following hold:*

- *If $B \supset A$, then $B \cap \Pi$ is a line of $\mathcal{P}_2(4)$.*
- *If $|B \cap A| = 2$, then $B \cap \Pi$ is a hyperoval.*
- *If $|B \cap A| = 1$, then $B \cap \Pi$ is a Fano plane.*
- *If $B \cap A = \emptyset$, then $B \cap \Pi$ is a* **double line** *(union of two lines, with the point of intersection omitted).*

Proof: The first case is clear. Let $|B \cap A| = 2$. It follows from the block intersection numbers that each line meets the 6-set $B \cap \Pi$ in 0 or 2 points. It follows that $B \cap \Pi$ is a hyperoval.
Let $|B \cap A| = 1$. The block intersection numbers show that each line meets the 7-set $E = B \cap \Pi$ in 1 or 3 points. It follows that the incidence structure induced by the lines on E is an $S(2,3,7)$, a Fano plane. Let finally $B \subset \Pi$. We see that every point $P \in B$ is on exactly one line meeting B in four points.■

This limits the number of 8-sets from which to choose the blocks of our design. In fact, the number of candidates is $21 + 168 + 360 + \binom{21}{2} = 759$. As this happens to be the number of blocks of an $S(5,8,24)$ we do not have much choice.

Definition (4.10) *Label the* G_0-*orbits* $\mathcal{Q}_i$ *of quadrangles,* $\mathcal{X}_i$ *of hyperovals and* $\mathcal{E}_i$ *of Fano planes such that the following hold:*

- *If* $Q \in \mathcal{Q}_i, Q \subset E, E$ *a Fano plane, then* $E \in \mathcal{E}_i$.
- *If* $Q \in \mathcal{Q}_i, Q \subset X, X$ *a hyperoval, then* $X \in \mathcal{X}_i$.

We define blocks to be all the 8-sets as follows:

1. $A \cup l$, *where* l *is a line of* $\mathcal{P}_2(4)$.
2. $\{a_i, a_j\} \cup X$, *where* X *is a hyperoval from* $\mathcal{X}_k$ *and* $\{i, j, k\} = \{1, 2, 3\}$.
3. $\{a_i\} \cup E$, *where* E *is a Fano plane from from* $\mathcal{E}_i$.
4. *All 210 double lines*

Theorem (4.18) *The design constructed in Definition (4.10) is an* $S(5, 8, 24)$.

Proof: As we have used the right number 759 of blocks it suffices to prove that any 5-set $Y \subset \Omega = A \cup \Pi$ is in at least one block.
If $Y \supset A$, then Y is on a block of the first type. Let $Y \cap A = \{a_1, a_2\}$. We can assume that the points from $Y \cap \Pi$ form a triangle. By Lemma (4.13) a triangle is contained in (exactly one) hyperoval from orbit $\mathcal{X}_3$.
Let $Y \cap A = \{a_1\}$. We are done if the four points of $Y \cap \Pi$ are either collinear or from a quadrangle. The only other possibility is that they from what we may a **double triangle:** three points on a line l, the fourth point off l. The usual type of double counting argument shows that G_0 is regular on double triangles and that each double triangle is in eactly three Fano planes, one from each orbit.
Remains the case $Y \subset \Pi$. We are done if some four points are collinear (= on a line) or if no three points are collinear (the hyperoval case). So let P, Q, R be collinear on line l, and S, T the two remaining points. If line ST intersects l in P, Q or R, then Y is contained in a Fano plane. If not, then Y is in a double line.∎

This Theorem, together with the block intersection numbers of Lemma (4.14), gives us additional information on the structure of $\mathcal{P}_2(4)$:

Lemma (4.16) • *Two hyperovals are in the same G_0-orbit if and only they they intersect in even cardinality (0 or 2).*

- *Two Fano planes are in the same $G-0-$orbit if and only if they intersect in odd cardinality (1 or 3).*
- *A hyperoval and a Fano plane have quadrangles from the same $G-0-$orbit if and only they intersect in even cardinality (0,2 or 4).*

We conclude that $S(5,8,24)$ is uniquely determined up to isomorphism. In fact, the derived design of an $S(5,8,24)$ with respect to three points is an $S(2,5,21)$ or projective plane of order 4, which by Problem (4.10) is uniquely determined. We know from Lemma (4.15) the intersections $B \cap \Pi$ of all the blocks. Lemma (4.16) shows that B is always uniquely determined by $B \cap \Pi$, up to a permutation of A.

Theorem (4.19) *There is up to isomorphism exactly one design $S(5,8,24)$, the* **large Witt design.**

The situation is so tight that we can determine the automorphism group of this design. Denote by M_{24} the automorphism group of the large Witt design and by M_{24-i} the pointwise stabilizer of i points, $i = 1,2,3,4,5$. The construction shows that M_{24} is 3-transitive. As by construction $M_{21} \geq G_0 = PSL_3(4)$ we see that M_{21} is still 2-transitive on the remaining 21 points. It follows that M_{24} is 5-transitive and $|M_{24}| = 24 \cdot 23 \cdot 22 \cdot |M_{21}| \geq 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$. Fix a set A of three points. Let H be the set-stabilizer of A in M_{24}. It follows $|M_{24}| = \frac{24 \cdot 23 \cdot 22}{6}|H|$. On the other hand $H \leq Aut(\mathcal{P}_2(4))$. We know the group $G = PGL_3(4) \leq Aut(\mathcal{P}_2(4))$, which is transitive on hyperovals and induces A_6 on a hyperoval. As the stabilizer of a hyperoval in $Aut(\mathcal{P}_2(4))$ must clearly by faithfully represented on the hyperoval and can therefore be at most S_6 we conclude that $Aut(\mathcal{P}_2(4))$ can be at most double as big as G. It follows $|M_{24}| \leq 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$. We must have equality.

Theorem (4.20) *The full automorphism group of the $S(5,8,24)$ is a 5-transitive group M_{24} (the* **large Mathieu group***) of order*

$$|M_{24}| = 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48.$$

The stabilizer of three points is the simple group $PSL_3(4)$.

As a corollary we see that the full automorphism group of $\mathcal{P}_2(4)$ has order $2^7 \cdot 3^3 \cdot 5 \cdot 7$ and induces the full symmetric group S_6 on each hyperoval.

Theorem (4.21) *$M_{24}, M_{23}, M_{22}, M_{21}$ are simple groups*

Proof: We know that $M_{21} \cong PSL_3(4)$ is simple (Theorem (4.16)). Let us show that M_{22} is simple. If this is not the case, then by Theorem (2.4) M_{22} contains a regular normal subgroup N (of order 22). Let $H \cong M_{21}$ be the stabilizer of a point. Then $M_{22} = HN$. Let H act on N by conjugation. As $Aut(N)$ is solvable and H is simple, we conclude that H must induce the identity group on N. It follows $[H, N] = 1$ and $H \lhd M_{22}$. Conjugation under N shows that H fixes every point, hence $H = 1$, contradiction. We have proved that M_{22} is a simple group.
The same argument proves that M_{23} and M_{24} are simple.■

4.11 The binary Golay code and the small Witt designs

Definition (4.11) (codes) *A* **linear code** *over $\mathbb{F}_q$ is a subspace $\mathcal{C}$ of the vector space $\mathbb{F}_q^n$ of n-tuples. Its* **minimum distance** *d is the largest number such that any two different elements of $\mathcal{C}$ differ in at least d coordinates. The* **(Hamming) weight** *$wt(v)$ is the number of coordinates, where v has nonzero entry. The parameters of such a code are recorded as*

$$[n, k, d]_q$$

(n is the **length**, *k the dimension). For $x, y \in \mathbb{F}_q^n$ consider the scalar product $x \cdot y = \sum_{i+1}^{n} x_i y_i$. As this is nondegenerate the* **dual code** *$\mathcal{C}^\perp = \{y | x \cdot y = 0$ for all $x \in \mathcal{C}\}$ has dimension $n - k$.*

Definition (4.12) (binary Golay code) *Identify the set Ω of points of $S(5, 8, 24)$ with a basis of $\mathbb{F}_2^{24}$ and identify each vector with its support. The code $\mathcal{G}$ generated by the blocks of $S(5, 8, 24)$ is the* **binary Golay code.** *The 759 vectors corresponding to blocks will be called* **octads.**

The blocks of the Witt design constitute 759 vectors of weight 8. We ask what the dimension d and minimum distance k of $\mathcal{G}$ are. As all the block intersections are even (Lemma (4.14)) we conclude that $\mathcal{G} \subseteq \mathcal{G}^{\perp}$. In particular $k \leq 12$. As every point $P \in \Omega$ is in precisely 253 blocks we see that the sum over all octads is the all-1-vector $\mathbf{1} = (1, 1, 1, \ldots)$. Consider the factor space $\mathcal{G}/ < \mathbf{1} >$, of dimension $k-1$. The group M_{24} in its operation as a permutation group of the coordinates operates as a group of linear mappings on this space. As M_{24} is simple we see that $M_{24} \leq GL_{k-1}(2)$. We know that 23 divides the order of M_{24} and we can compare with the orders of the linear groups. As 23 does not divide $2^i - 1$ for any $0 \leq i < 11$ we conclude that $k - 1 \geq 11$ and hence $k = 12$. It follows $\mathcal{G} = \mathcal{G}^{\perp}$.

Problem (4.12) *Prove the following: If x, y are binary vectors of the same length, both of weight divisible by four and with even intersection (the number of coordinates where both x and y has entry 1 is even), then $x + y$ has weight divisible by four.*

Definition (4.13) *Let $\mathcal{C}$ be a code $[n, k, d]_q$. Denote by A_i the number of vectors $v \in \mathcal{C}$ having weight i.*

Clearly $A_0 = 1$ and $A_i = 0$ for $0 < i < d$. Also $\sum_i A_i = |\mathcal{C}| = q^k$.
Back to the binary Golay code. We know that all weights are multiples of 4 (Problem (4.12)). The presence of the all-1 vector shows not only $A_{24} = 1$ but also $A_{24-i} = A_i$ for all i. We claim that $A_4 = 0$. In fact, let $Q \subset \Omega$ be a subset of cardinality 4, which is in $\mathcal{G}$. Choose a block (octad) intersecting Q in precisely three points. This contradicts the fact that $\mathcal{G}$ is self-dual. In the same spirit it is easy to see that the blocks are the only vectors of weight 8. In fact, let $X \subset \Omega$ be of cardinality eight and contained in $\mathcal{G}$. Choose a block meeting X in at least 5 (hence in at least 6) points. Because of linearity $X + B$ also is a code-word. As its weight is ≤ 4, it is the 0-word, thus $X = B$. We have proved $A_4 = A_20 = 0, A_8 = A_{16} = 759, A_0 = A_{24} = 1$. As $\sum_i A_i = 2^{12}$, we see that A_{12} is uniquely determined as well.

Theorem (4.22) *The binary Golay code $\mathcal{G}$ has parameters* $[24, 12, 8]$. *It is self-dual ($\mathcal{G} = \mathcal{G}^{\perp}$) and has weight distribution*

$$A_0 = A_{24} = 1, A_8 = A_{16} = 759, A_{12} = 2576.$$

The codewords of weight 12 of the binary Golay code (or their supports) are called **dodecads.** Let D be a dodecad, $T \subset D$ a 5-set, $B \supset T$ the unique block containing it. As B must meet D in even cardinality and cannot be contained in D ($B + D$ would have weight 4 otherwise), we conclude $|B \cap D| = 6$. This shows that we obtain a Steiner system $S(5, 6, 12)$.

Theorem (4.23) (small Witt design) *Let D be a dodecad (word of weight 12) of the binary Golay code. The family of 6-subsets of D, which are contained in octads, form the block of a design $S(5, 6, 12)$.*

We see that the binary Golay code contains 2576 copies of design, which have the parameters of the small Witt design.

Bibliography

[1] W.O.Alltop: *An infinite class of 4-designs,* Journal of Combinatorial *Theory* **6** (1969),320-322.

[2] N.L. Biggs, White, *Permutation groups and combinatorial structures,* Cambridge University Press 1979.

[3] N.G. de Bruijn, *Pólyas Abzähl-Theorie: Muster für Graphen und chemische Verbindungen,* Selecta Mathematica *III* 1-26 (K. Jakobs, ed), Springer 1971.

[4] D. Hughes, F. Piper, *Design Theory,* Cambridge University Press 1985.

[5] A. Kerber, Bayreuther Mathematische Schriften **12**(1983),**15** (1983),**21**(1986).

[6] A. Kerber, *Algebraic Combinatorics via Finite Group Actions,* BI Mannheim.

[7] Moore, *Tactical Memoranda,* American Journal of Mathematics **18** (1896), 268-275.

[8] Netto, *Lehrbuch der Kombinatorik*, ^{2}1927, with notes by Skolem in the appendix.

[9] G. Pólya, *Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen,* Acta Mathematika **68** (1937), 145-254.

[10] E. Witt, *Über Steinersche Systeme,* Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **12**(1938),265-275.

[11] Richard M. Wilson, *Some partitions of all triples into Steiner triple systems,* Proceedings of the Hypergraph Seminar, Ohio State University 1972, *Lecture Notes in Mathematics* **411** (C. Berge, Ray-Chaudhury, eds) 1974, 267-277.