Intense automorphisms of finite groups

Stanojkovski, M.

Chapter 1

Important tools

This chapter consists of a miscellaneous collection of definitions and easy facts. Throughout the whole chapter we will fully respect the notation given in the List of Symbols.

1.1 Bilinear maps and isotropic spaces

Let K be a field and let V, W, and Z be vector spaces over K. A map $\phi : V \times W \to Z$ is said to be *K-bilinear* (or simply *bilinear*) if, for all $v \in V$, the map ${}_v\phi : W \to Z$, defined by $t \mapsto \phi(v,t)$, is K-linear and, for all $w \in W$, the map $\phi_w : V \to Z$, defined by $u \mapsto \phi(u,w)$, is K-linear.

Definition 1. *Let V, W, and Z be vector spaces over a field K and let $\phi : V \times W \to Z$ be a map. Then ϕ is* non-degenerate *if it is bilinear and both maps $V \to \mathrm{Hom}(W,Z)$, defined by $v \mapsto {}_v\phi$, and $W \to \mathrm{Hom}(V,Z)$, defined by $w \mapsto \phi_w$, are injective.*

Lemma 2. *Let V, W, Z be finite-dimensional vector spaces over a field K and let $\phi : V \times W \to Z$ be a non-degenerate map. Assume moreover that $\dim_K Z = 1$. Then the dimensions of V and W over K are the same.*

Proof. The maps $V \to \mathrm{Hom}(W,Z)$ and $W \to \mathrm{Hom}(V,Z)$ are injective. It follows that $\dim V \leq \dim \mathrm{Hom}(W,Z) = \dim W \leq \dim \mathrm{Hom}(V,Z) = \dim V$, and therefore the dimensions of V and W are the same. ∎

Definition 3. *Let V and Z be vector spaces over a field K. A map $\phi : V \times V \to Z$ is* alternating *if it is bilinear and, for all $v \in V$, one has $\phi(v,v) = 0$.*

A map $\phi : V \times V \to Z$ is *antisymmetric* if it is bilinear and, for every $v, w \in V$ one has $\phi(v,w) = -\phi(w,v)$. As a direct consequence of their definitions, every alternating map is antisymmetric.

Lemma 4. *Let K be a field and let U be a K-vector space of dimension 3. Then $\wedge : U \times U \to \bigwedge^2 U$ is surjective.*

Proof. Let (x, y, z) be a basis for U over K. Then $(x \wedge y, y \wedge z, x \wedge z)$ is a basis for $\bigwedge^2 U$. Let now $a = \lambda(x \wedge y) + \mu(y \wedge z) + \nu(x \wedge z)$ be an arbitrary element of $\bigwedge^2 U$. If $a = 0$, then clearly a belongs to the image of $\wedge$, so, without loss of generality, we assume that $\lambda \in K \setminus \{0\}$. Since $(\lambda x - \mu z) \wedge (y + \lambda^{-1}\nu z) = a$, we are done. ∎

Definition 5. *Let K be a field and let V and Z be vector spaces over K. Let $\phi : V \times V \to Z$ be an alternating map. A subspace T of V is called* isotropic *if ϕ restricted to $T \times T$ equals the zero map. A subspace T is said to be* maximal isotropic *if it is isotropic and it is not properly contained in any other isotropic subspace of V.*

Definition 6. *Let K be a field and let V and Z be vector spaces over K. Let $\phi : V \times V \to Z$ be an alternating map and let T be an isotropic subspace of V. Then $\phi_T : V/T \to \mathrm{Hom}(T, Z)$ is defined by $v + T \mapsto (t \mapsto \phi(v, t))$.*

The map ϕ_T is well defined for every isotropic subspace T of V, because $\phi(T \times T) = 0$, and it is linear.

Lemma 7. *Let K be a field and let V and Z be vector spaces over K. Let $\phi : V \times V \to Z$ be an alternating map and let T be an isotropic subspace of V. Then T is maximal isotropic if and only if ϕ_T is injective.*

Proof. The subspace T is not maximal isotropic if and only if there exists an element $v \in V \setminus T$ such that $T \oplus Kv$ is isotropic, which happens if and only if $v + T$ belongs to the kernel of ϕ_T. ∎

Definition 8. *Let K be a field and let V and Z be vector spaces over K. Let $\phi : V \times V \to Z$ be an alternating map. Let moreover W be a linear subspace of V. The* orthogonal complement *$W^\perp$ of W with respect to ϕ is the kernel of the map $V \to \mathrm{Hom}(W, Z)$ that is defined by $v \mapsto (w \mapsto \phi(v, w))$.*

With the notation of Definition 8, the orthogonal complement of a subspace W of V is itself a subspace of V. Moreover, an alternating map being antisymmetric, $W^\perp$ is equal to the collection of all vectors $v \in V$, such that, for all $w \in W$, one has $\phi(w, v) = 0$. It follows directly from the definition that $W \subseteq (W^\perp)^\perp$ and that, if $U \subseteq W$, then $U^\perp \supseteq W^\perp$.

Lemma 9. *Let K be a field and let V and Z be vector spaces over K. Let $\phi : V \times V \to Z$ be an alternating map. Let moreover W be a linear subspace of V. Then W is isotropic if and only if $W \subseteq W^\perp$. Moreover, W is maximal isotropic if and only if $W = W^\perp$.*

Proof. Easy exercise. ∎

Lemma 10. *Let V and Z be finite-dimensional vector spaces over a field K and let $\phi : V \times V \to Z$ be a non-degenerate alternating map. Assume that Z has dimension 1. Let W be a linear subspace of V. Then $\dim W + \dim W^\perp = \dim V$. Moreover, if W is maximal isotropic, then $2 \dim W = \dim V$.*

Proof. By definition of orthogonal complement, we have $\phi(W^\perp \times W) = \{0\}$, and hence the bilinear map $V/W^\perp \times W \to Z$ that is induced from ϕ is non-degenerate. It follows from Lemma 2 that $\dim V - \dim W^\perp = \dim W$. If W is maximal isotropic, then Lemma 9 yields $\dim V = 2 \dim W$. ∎

Lemma 11. *Let V and Z be finite-dimensional vector spaces over a field K and let $\phi : V \times V \to Z$ be a non-degenerate alternating map. Assume that Z has dimension 1. Let W be a linear subspace of V. Then $(W^\perp)^\perp = W$.*

Proof. The subspace W is always contained in $(W^\perp)^\perp$, and therefore we always have $\dim W \leq \dim(W^\perp)^\perp$. By Lemma 10, the dimension of V is equal to both $\dim W + \dim W^\perp$ and $\dim W^\perp + \dim(W^\perp)^\perp$, and therefore $\dim W = \dim(W^\perp)^\perp$. It follows that $W = (W^\perp)^\perp$. ∎

Lemma 12. *Let V and Z be finite-dimensional vector spaces over a field K and let $\phi : V \times V \to Z$ be a non-degenerate alternating map. Assume that Z has dimension 1. Let moreover X be a maximal isotropic subspace of V. Then there exists a maximal isotropic subspace Y of V such that $V = X \oplus Y$.*

Proof. Let Y be maximal among the isotropic subspaces of V that intersect X trivially. We will show that Y is maximal isotropic and that $V = X + Y$. Lemma 9 guarantees $Y \subseteq Y^\perp$ and $X = X^\perp$. We now claim that $Y^\perp$ is contained in $X + Y$. Indeed, if $v \in Y^\perp$, then $Y + Kv$ is an isotropic subspace containing Y. From the maximality of Y, it follows that $(Y + Kv) \cap X$ is non-trivial. Since $Y \cap X = \{0\}$, the element v belongs to $X + Y$, as claimed. Now, by Lemma 11, the subspaces $(Y^\perp)^\perp$ and Y are the same and, $Y^\perp$ being contained in $X + Y$, it follows that

$$Y = (Y^\perp)^\perp \supseteq (X + Y)^\perp \supseteq X^\perp \cap Y^\perp = X \cap Y^\perp.$$

In particular, $X \cap Y^\perp$ is contained in $X \cap Y$, which is trivial by definition of Y. As a consequence of Lemma 10, we get that

$$2 \dim X = \dim V \geq \dim(X \oplus Y^\perp) = \dim X + \dim Y^\perp =$$

$$\dim X + \dim V - \dim Y = 3 \dim X - \dim Y \geq 2 \dim X,$$

and therefore $\dim Y^\perp = \dim X = \dim Y$. As a result, $Y = Y^\perp$, and thus $V = X \oplus Y$. The subspace Y is maximal isotropic, by Lemma 9, and the proof is complete. ∎

1.2 Commutators and the lower central series

Let G be a group. The *commutator map* on G is the map $G \times G \to G$ that is defined by

$$(x, y) \mapsto [x, y] = xyx^{-1}y^{-1}.$$

Given two subgroups H and K of G, we define $[H, K]$ to be the subgroup of G that is generated by all elements $[h, k]$, where $h \in H$, $k \in K$. The groups $[H, K]$ and $[K, H]$ are equal, because, for all $(h, k) \in H \times K$, the inverse of $[h, k]$ is $[k, h]$.

Lemma 13. *Let G be a group and let H be a subgroup of G. Let $g \in G$ and denote $[g, H] = \{[g, h] \ : \ h \in H\}$. Then $g \in \mathrm{N}_G(H)$ if and only if $[g, H]$ is contained in H.*

Proof. Let $h \in H$. Then $ghg^{-1} = [g, h]h$ and ghg^{-1} is in H if and only if $[g, h]$ is in H. ∎

Definition 14. *Let G be a group. The* lower central series *of G is the series $(G_i)_{i\geq 1}$ that is obtained by defining recursively, for all $i \in \mathbb{Z}_{\geq 1}$, the subgroups $G_1 = G$ and $G_{i+1} = [G, G_i]$. One calls G_2 the* commutator subgroup *of G.*

Unless otherwise specified, we will stick to the notation from Definition 14 to refer to the lower central series of a group (see also the List of Symbols). We remark that, in Chapter 13, we will define the lower central series of a profinite group G, by taking the closures of the elements of the lower central series of G as an abstract group. In the case of finite groups, the two notions coincide.

A group G is said to be *nilpotent* if there exists $i \in \mathbb{Z}_{\geq 0}$ for which $G_{i+1} = 1$ and, in the latter case, one calls $\mathrm{cl}(G) = \min\{i \in \mathbb{Z}_{\geq 0} \ : \ G_{i+1} = 1\}$ the (*nilpotency*) *class* of G. The class of a nilpotent group is, in other words, the number of elements of the lower central series that are distinct from $\{1\}$. Another way of deciding whether a group is nilpotent is by looking at its upper central series.

Definition 15. *Let G be a group. The* upper central series *of G is the series $(Z_i)_{i\geq 0}$ that is obtained by defining recursively, for all $i \in \mathbb{Z}_{\geq 0}$, the subgroups $Z_0 = 1$ and $Z_{i+1}/Z_i = \mathrm{Z}(G/Z_i)$.*

It is a general result (see for example Chapter 4 in [Isa08]) that a group is nilpotent if and only if its upper central series stabilizes at the group itself. In other words, if G is a finite group and $(Z_i)_{i\geq 0}$ is its upper central series, then G is nilpotent if and only if there exists $r \in \mathbb{Z}_{\geq 0}$ such that $Z_r = G$. Moreover, one can show (see for example in [Isa08, §1D]) that if the group G is nilpotent, then its class is equal to $\min\{r \in \mathbb{Z}_{\geq 0} \ : \ Z_r = G\}$.

Lemma 16. *Let G be a finite group. Then G is nilpotent if and only if G is equal to the direct product of its Sylow p-subgroups.*

Proof. This is a weaker version of Hauptsatz 2.3 from [Hup67, Ch. III]. ∎

Definition 17. *Let G be a group and let m, n be integers with $m \leq n$. Let moreover $\{x_i\}_{i=m}^{n}$ be a subset of G. Then*

$$\prod_{i=m}^{n} x_i = x_m x_{m+1} \dots x_{n-1} x_n.$$

Lemma 18 (Multiplication formulas)**.** *Let G be a group and let x, y, z, t be elements of G. Let moreover n be a non-negative integer. Then the following hold.*

1. $[x, yz] = [x, y]y[x, z]y^{-1}$.
2. $[xt, y] = x[t, y]x^{-1}[x, y]$.
3. $[x^n, y][x, y]^{-n} = \prod_{s=1}^{n-1}[x, [x^{n-s}, y]]$.
4. $[x, y]^{-n}[x, y^n] = \prod_{r=1}^{n-1}[[y^r, x], y]$.

Proof. Easy exercise. ∎

Lemma 19 (Three-subgroups Lemma)**.** *Let G be a group and let X, Y, Z, and N be subgroups of G such that N is normal. Assume moreover that both $[X, [Y, Z]]$ and $[Y, [Z, X]]$ are contained in N. Then $[Z, [X, Y]]$ is contained in N.*

Proof. See for example [Isa08, Corollary 4.10]. ∎

Lemma 20. *Let G be a group and let $(G_i)_{i\geq 1}$ be the lower central series of G. Then, for all $h, k \in \mathbb{Z}_{\geq 1}$, one has $[G_h, G_k] \subseteq G_{h+k}$.*

Proof. We work by induction on h. If $h = 1$, we are done by definition of the lower central series. Let us now assume that $h > 1$ and, for all $k \in \mathbb{Z}_{>0}$, that $[G_{h-1}, G_k] \subseteq G_{h+k-1}$. It follows that $[G, [G_{h-1}, G_k]] \subseteq [G, G_{h+k-1}] \subseteq G_{h+k}$ and $[G_{h-1}, [G_k, G]] \subseteq [G_{h-1}, G_{k+1}] \subseteq G_{h+k}$. By Lemma 19, also $[G_h, G_k] = [[G, G_{h-1}], G_k]$ is contained in G_{h+k}. ∎

Let H, K, and L be groups. Let moreover $\phi : H \times K \to L$. The map ϕ is *bilinear* if, for all $h \in H$, the map ${}_h\phi : K \to L$, defined by $x \mapsto \phi(h, x)$, is a homomorphism and, for all $k \in K$, the map $\phi_k : H \to L$, defined by $x \mapsto \phi(x, k)$, is also a homomorphisms. If ϕ is bilinear, then the *left kernel* and the *right kernel* of ϕ, are defined as

$$\ker^{\text{left}} \phi = \bigcap_{h\in H} \ker {}_h\phi, \quad \text{and} \quad \ker^{\text{right}} \phi = \bigcap_{k\in K} \ker \phi_k.$$

Assume $H = K$. Then ϕ is *alternating* if it is bilinear and, for all $x \in H$, one has $\phi(x, x) = 1$.

Definition 21. *Let H, K, and L be groups. Let moreover $\phi : H \times K \to L$. Then ϕ is* non-degenerate *if it is bilinear and both maps $H \to \mathrm{Hom}(K, L)$, defined by $h \mapsto {}_h\phi$, and $K \to \mathrm{Hom}(H, L)$, defined by $k \mapsto \phi_k$, are injective.*

Lemma 22. *Let G be a group and let H, L be subgroups of G. Let moreover $\phi : H \times L \to G$ be defined by $\phi(x, y) = [x, y]$. Then ϕ is bilinear if and only if $[H, L]$ is contained in the centre of the subgroup generated by H and L.*

Proof. This follows directly from the multiplication formulas from Lemma 18. ∎

Lemma 23. *Let G be a group. Then for every $h, k \in \mathbb{Z}_{\geq 1}$ the commutator map induces a bilinear map $G_h/G_{h+1} \times G_k/G_{k+1} \to G_{h+k}/G_{h+k+1}$.*

Proof. The integers h and k being positive, it follows from Lemma 20 that both $[G_h, G_{h+k}]$ and $[G_k, G_{h+k}]$ are subgroups of G_{h+k+1}. Then G_{h+k}/G_{h+k+1} is contained in the centre of $\langle G_h, G_k\rangle/G_{h+k+1}$ and, by Lemma 22, the commutator map $G_h \times G_k \to G_{h+k}/G_{h+k+1}$ is bilinear. Again by Lemma 20, both subgroups $[G_h, G_{k+1}]$ and $[G_{h+1}, G_k]$ are contained in G_{h+k+1}. The commutator map induces hence a bilinear map $G_h/G_{h+1} \times G_k/G_{k+1} \to G_{h+k}/G_{h+k+1}$. ∎

Lemma 24. *Let G be a group. Then for every $i \in \mathbb{Z}_{\geq 1}$ the commutator map induces a bilinear map $G/G_2 \times G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ whose image generates G_{i+1}/G_{i+2}.*

Proof. The commutator map induces a bilinear map $\gamma : G/G_2 \times G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ by Lemma 23. The image of γ generates G_{i+1}/G_{i+2} by definition of the lower central series of a group. ∎

In Lemma 25 and throughout the whole manuscript, we write $\otimes$ instead of $\otimes_{\mathbb{Z}}$ (in concordance with the List of Symbols).

Lemma 25. *Let G be a group and let $(G_i)_{i\geq 1}$ be its lower central series. Then for every $i \in \mathbb{Z}_{\geq 1}$ the commutator map induces a surjective homomorphism of groups $G/G_2 \otimes G_i/G_{i+1} \to G_{i+1}/G_{i+2}$.*

Proof. This follows from Lemma 24 and the universal property of tensor products. ∎

Lemma 26. *Let G be a group of class at most 2. Then the commutator map induces a non-degenerate alternating map $G/\operatorname{Z}(G) \times G/\operatorname{Z}(G) \to G_2$ whose image generates G_2.*

Proof. By Lemma 24, the commutator map induces a bilinear map $\gamma : G/G_2 \times G/G_2 \to G_2$ whose image generates G_2. Moreover, γ is alternating because each element of G commutes with itself. The class of G being at most 2, the subgroup G_2 is central and $\operatorname{Z}(G)/G_2$ is equal to both the right and the left kernel of γ. Then γ factors as a non-degenerate map $G/\operatorname{Z}(G) \times G/\operatorname{Z}(G) \to G_2$. ∎

Lemma 27. *Let G be a group and assume that $G/\operatorname{Z}(G)$ is cyclic. Then G is abelian.*

Proof. Since the quotient $G/\operatorname{Z}(G)$ is cyclic, the commutator subgroup of G is contained in $\operatorname{Z}(G)$. In particular, G has class at most 2, and therefore, thanks to Lemma 26, the commutator map induces a non-degenerate alternating map $\gamma : G/\operatorname{Z}(G) \times G/\operatorname{Z}(G) \to G_2$ whose image generates G_2. The image of γ is trivial, because $G/\operatorname{Z}(G)$ is cyclic, and so $G = \operatorname{Z}(G)$. ∎

Lemma 28. *Let G be a group and let N be a normal subgroup of G. Assume that G/N is cyclic. Then $G_2 = [G, N]$.*

Proof. Since N is normal, the subgroup $[G, N]$ is normal in G. We denote by $\overline{G} = G/[G, N]$ and we use the bar notation for the subgroups of $\overline{G}$. By definition of $\overline{G}$, the subgroup $\overline{N}$ is contained in $\operatorname{Z}(\overline{G})$, and so $\overline{G}/\operatorname{Z}(\overline{G})$ is cyclic. It follows from Lemma 27 that $\overline{G}$ is abelian, and therefore $G_2 = [G, N]$. ∎

1.3 About p-groups

Let p be a prime number. A finite group G is a *p-group* if the order of G is a power of p. The trivial group is a p-group for each prime p. Moreover, as a direct consequence of Lemma 16, every finite p-group is nilpotent.

Lemma 29. *Let p be a prime number and let G be a finite p-group. Let N be a normal subgroup of G such that $N \cap \operatorname{Z}(G) = \{1\}$. Then $N = \{1\}$.*

Proof. This is Satz 7.2(a) from [Hup67, Ch. III]. ∎

Lemma 30. *Let p be a prime number and let G be a finite p-group of class c. Let moreover N be a subgroup of G. Assume that, for all $i \in \{1, \dots, c\}$, if H is a quotient of G of class i, then $\operatorname{Z}(H) = H_i$. Then N is normal if and only if there exists $i \in \mathbb{Z}_{>0}$ such that $G_{i+1} \subseteq N \subseteq G_i$.*

Proof. ($\Leftarrow$) Assume that $G_{i+1} \subseteq N \subseteq G_i$. Then the quotient N/G_{i+1} is contained in $\operatorname{Z}(G/G_{i+1})$, and so N is normal modulo G_{i+1}. In particular, N is normal in G. ($\Rightarrow$) If $N = \{1\}$, the result is clear, because G is nilpotent. We assume N is a non-trivial normal subgroup of G and we let $i \in \mathbb{Z}_{>0}$ be the minimum index such that $G_{i+1} \subseteq N$ and $G_{i+1} \neq N$. We claim that N is contained in G_i. First assume that G_i is contained in N. By the minimality of i, the subgroup G_i is equal to N, so we are done with this case. We assume now that G_i is not contained in N. Then the group $\overline{G} = G/(N \cap G_i)$ has class i and, by assumption, the center of $\overline{G}$ is equal to $\overline{G_i}$. On the other hand, $\overline{N}$ is a normal subgroup of $\overline{G}$ that has trivial intersection with $\overline{G_i}$. Lemma 29 yields $\overline{N} = \{1\}$, and thus $N \subseteq G_i$. ∎

Lemma 31. *Let p be a prime number and let G be a finite p-group. Assume that G/G_2 is cyclic. Then G is abelian.*

Proof. This is a weaker version of Hilfssatz 7.1(b) from [Hup67, Ch. III.7]. ∎

Definition 32. *Let G be a group. Then, for all $n \in \mathbb{Z}$, define*

$$G^n = \langle x^n \ : \ x \in G \rangle \quad \text{and} \quad \mu_n(G) = \langle x \in G \ : \ x^n = 1 \rangle.$$

Let p be a prime number. The *Frattini subgroup* $\Phi(G)$ of a finite p-group G is the unique normal subgroup of G minimal with the property that $G/\Phi(G)$ is elementary abelian: in other words $\Phi(G) = G^p[G, G]$.

Lemma 33. *Let p be a prima number and let G be a finite p-group. Let H be a subgroup of G such that $G = H\Phi(G)$. Then $H = G$.*

Proof. This is a weaker reformulation of Satz 3.2(a) from [Hup67, Ch. III]. ∎

Lemma 34. *Let p be a prime number and let G be a finite p-group. Then the map $\phi : \mathrm{Aut}(G) \to \mathrm{Aut}(G/\Phi(G))$ given by $\alpha \mapsto (x\Phi(G) \mapsto \alpha(x)\Phi(G))$ is a well-defined homomorphism. Moreover, the kernel of ϕ is a p-group.*

Proof. This is a reformulation of Satz 3.18 from [Hup67, Ch. III]. ∎

Lemma 35. *Let p be a prime number and let H be a finite p-group. Let moreover K and N be normal subgroups of H such that $K \subseteq N$ and $K \neq N$. Then there exists a normal subgroup M of H such that $K \subseteq M \subseteq N$ and $|N : M| = p$.*

Proof. See [Isa08, Lemma 1.23]. ∎

Lemma 36. *Let p be a prime number and let G be a finite p-group. Assume that $|G : G_2| = p^2$. Then one of the following holds.*

1. *The group G is abelian.*
2. *The group G_2 is equal to $\Phi(G)$.*

Proof. Assume that G is not abelian. It follows from Lemma 31 that G/G_2 has exponent p and so G^p is contained in G_2. In particular, we have that $G_2 = G_2G^p = \Phi(G)$. ∎

Definition 37. *Let G be a group and let p be a prime number. The* p-central series *of G is the series $(P_i(G))_{i \geq 1}$ that is obtained by defining recursively, for all $i \in \mathbb{Z}_{\geq 1}$, the subgroups $P_1(G) = G$ and $P_{i+1}(G) = [G, P_i(G)]P_i(G)^p$.*

We remark that, if p is a prime number and G is a finite p-group, then saying that the lower central series of G coincides with its p-central series is equivalent to saying that all quotients of consecutive elements of the lower central series have exponent dividing p.

1.4 Extraspecial p-groups

In Section 1.4 we explore the world of extraspecial p-groups, a class of groups that have been widely studied and whose structure is very well-understood (see for example [Hup67, Ch. III.13]). Given a group G, we recall that $(G_i)_{i\geq 1}$ denotes its lower central series (see Section 1.2).

Definition 38. *Let p be a prime number and let G be a finite p-group. Then G is* extraspecial *if G_2 is central and $\mathrm{Z}(G)$ is cyclic of order p.*

Lemma 39. *Let p be a prime number and let G be a finite extraspecial p-group. If G is non-abelian, then $\mathrm{Z}(G)$ and G_2 are equal and they both have order p.*

Proof. Straightforward. ∎

Lemma 40. *Let p be a prime number and let G be a finite p-group. Assume that G has class at most 2 and that the exponent of G_2 divides p. Then $\Phi(G)$ is contained in $\mathrm{Z}(G)$.*

Proof. By Lemma 26, the map $G/\mathrm{Z}(G) \times G/\mathrm{Z}(G) \to G_2$ that is induced by the commutator map is bilinear. Let now $g, x \in G$. Then $[g^p, x] = [g, x]^p = [g, x^p]$ and $[g, x]^p = 1$, since the exponent of G_2 divides p. It follows that $G/\mathrm{Z}(G)$ is annihilated by p and thus $\Phi(G) \subseteq \mathrm{Z}(G)$. ∎

Lemma 41. *Let p be a prime number and let G be an extraspecial p-group. Then there exists $n \in \mathbb{Z}_{\geq 0}$ such that $|G| = p^{2n+1}$.*

Proof. This is a reformulation of Satz 13.7(c) from [Hup67, Ch. III]. ∎

Lemma 42. *Let p be a prime number and let X, Y, Z be finite-dimensional vector spaces over $\mathbb{F}_p$ such that $\dim_{\mathbb{F}_p} Z = 1$. Let moreover $\theta : X \times Y \to Z$ be a non-degenerate map. Call $G = G(Z, Y, X, \theta)$ the set $Z \times Y \times X$ together with the multiplication defined by $(z, y, x)(z', y', x') = (z + z' + \theta(x, y'), y + y', x + x')$. Then the following hold.*

1. *One has that G is an extraspecial p-group and, if p is odd, then G has exponent p.*
2. *The centre of G is $Z \times \{0\} \times \{0\}$.*
3. *The commutator map $G \times G \to G$ is given by*

$$((z, y, x), (z', y', x')) \mapsto [(z, y, x), (z', y', x')] = (\theta(x, y') - \theta(x', y), 0, 0).$$

Proof. Straightforward. ∎

Lemma 43. *Let p be a prime number and let G be an extraspecial p-group of exponent p. Then there exist finite-dimensional vector spaces X, Y, Z over $\mathbb{F}_p$, with Z of dimension 1, and a non-degenerate map $\theta : X \times Y \to Z$ such that $G \cong G(Z, Y, X, \theta)$.*

Proof. If G is abelian, we take $X = Y = 0$, $Z = G$, and θ to be the zero map. Since every group of exponent 2 is abelian, we are done when $p = 2$. Assume now that p is odd and that G has class 2. In this case $\mathrm{Z}(G) = G_2$ and $V = G/\mathrm{Z}(G)$ is a finite-dimensional vector space over $\mathbb{F}_p$, as a consequence of Lemma 40. Write $Z = \mathrm{Z}(G)$ and let $\pi : G \to V$ denote the canonical projection. By Lemma 26, the commutator map on G induces a non-degenerate map $\phi : V \times V \to Z$. Let now X be a maximal isotropic subspace of V. By Lemma 12 there exists an isotropic subspace Y of V such that $V = X \oplus Y$. It follows that the map $\phi_{|X\times Y} : X \times Y \to Z$ is non-degenerate. Now, we have that $0 = \phi(X \times X) = [\pi^{-1}(X), \pi^{-1}(X)]$, and so $\pi^{-1}(X)$ is abelian of exponent p. As a result, the sequence $0 \to Z \to \pi^{-1}(X) \to X \to 0$ of $\mathbb{F}_p$-modules is split and there is a homomorphism $s : X \to \pi^{-1}(X)$ such that $\pi \circ s = \mathrm{id}_X$. The same argument applies to Y and there exists therefore a homomorphism $t : Y \to \pi^{-1}(Y)$ such that $\pi \circ t = \mathrm{id}_Y$. To conclude, we denote $\theta = \phi_{|X\times Y}$ and we define $\psi : G(Z, Y, X, \theta) \to G$ by $(z, y, x) \mapsto zt(y)s(x)$. It is not difficult at this point to check that ψ is an isomorphism. ∎

Proposition 44. *Let p be a prime number. Let moreover X, Y, Z, A, B, C be finite-dimensional vector spaces over $\mathbb{F}_p$ with $\dim Z = \dim C = 1$. Let $\theta : X \times Y \to Z$ and $\psi : A \times B \to C$ be non-degenerate maps. Let f, g, h respectively belong to $\mathrm{Hom}(X, A), \mathrm{Hom}(Y, B), \mathrm{Hom}(Z, C)$ and assume that the following diagram is commutative.*

$$\begin{array}{ccc} X \times Y & \xrightarrow{\theta} & Z \\ {\scriptstyle f}\downarrow \quad \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} \\ A \times B & \xrightarrow{\psi} & C \end{array}$$

Then $(h, g, f) : G(Z, Y, X, \theta) \to G(C, B, A, \psi)$ is a homomorphism of groups and, if f, g, h are isomorphisms, then (h, g, f) is an isomorphism.

Proof. Straightforward. ∎

Lemma 45. *Let T be a group and let S be a central subgroup of T. Let moreover Δ denote the subgroup of $\mathrm{Aut}(T)$ consisting of all those elements δ such that $\delta(S) = S$ and such that δ induces the identity on both S and T/S. Then the map*

$$\Delta \to \mathrm{Hom}(T/S, S)$$

that is defined by

$$\delta \mapsto (xS \mapsto \delta(x)x^{-1})$$

is bijective.

Proof. Let $\phi : \Delta \to \mathrm{Hom}(T/S, S)$ denote the map $\delta \mapsto (xS \mapsto \delta(x)x^{-1})$, which is well-defined because S is central in T. The map ϕ is clearly injective and it is surjective because, given each homomorphism $f \in \mathrm{Hom}(T, S)$ with $S \subseteq \ker(f)$, the map $x \mapsto xf(x)$ belongs to Δ. ∎

Lemma 46. *Let p be a prime number and let G be an extraspecial p-group. Let Δ denote the subgroup of $\mathrm{Aut}(G)$ consisting of those automorphisms of G that induce the identity on G/G_2. Then $\Delta = \mathrm{Inn}(G)$.*

Proof. If G is abelian, then $\mathrm{Inn}(G)$ is trivial and we are done. Assume now that G is non-abelian. Then, by Lemma 39, the subgroups $\mathrm{Z}(G)$ and G_2 are equal and they both have order p. It follows from Lemma 26 that the commutator map induces a non-degenerate map $G/G_2 \times G/G_2 \to G_2$ and so the homomorphism $G/G_2 \to \mathrm{Hom}(G/G_2, G_2)$, defined by $t \mapsto (x \mapsto [t, x])$, is injective. Thanks to Lemma 40, the quotient G/G_2 is elementary abelian and thus $G/G_2 \to \mathrm{Hom}(G/G_2, G_2)$ is an isomorphism. Now, by Lemma 60, each element δ of Δ restricts to the identity on G_2 and so we derive from Lemma 45 that, for each element $\delta \in \Delta$, there exists $t \in G$ such that, for all $x \in G$, one has $\delta(x) = [t, x]x = txt^{-1}$. In particular, Δ is contained in $\mathrm{Inn}(G)$. The inclusion $\mathrm{Inn}(G) \subseteq \Delta$ is clear and so the proof is complete. ∎

1.5 Regular p-groups

Most of the results from this section are taken from [Hup67], an excellent reference for getting acquainted with regular p-groups. We recall here briefly the *Hall-Petrescu formula* and we refer to Appendix *A* from [DdSMS91] for more detail. We also refer to Definition 17 for a clear interpretation of the Hall-Petrescu formula.

Lemma 47 (Hall-Petrescu formula)**.** *Let G be a group and let $(G_i)_{i\geq 1}$ denote its lower central series. Let moreover x and y be elements of G. Then, for all $n \in \mathbb{Z}_{>0}$, there exists $(c_k)_{k=2}^n \in \prod_{k=2}^n G_k$ such that*

$$(xy)^n = x^n y^n \prod_{k=2}^{n} c_k^{\binom{n}{k}}.$$

Proof. See [DdSMS91, Appendix A]. ∎

Corollary 48. *Let p be a prime number and let G be a group. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. Then, for all $x, y \in G$, one has $(xy)^p \equiv x^p y^p \bmod G_2^p G_p$.*

Proof. This follows directly from Lemma 47. ∎

Definition 49. *Let p be a prime number. A finite p-group G is* regular *if, for all $x, y \in G$, there exists $\gamma \in [\langle x, y\rangle, \langle x, y\rangle]^p$ such that $(xy)^p = x^p y^p \gamma$.*

Lemma 50. *Let p be a prime number and let G be a finite p-group of nilpotency class at most $p-1$. Then G is regular.*

Proof. The class of each subgroup of G is at most that of G. The result now follows directly from Corollary 48. ∎

Let p be a prime number and let G be a p-group. We will denote by ρ the map $G \to G$ that is defined by $x \mapsto x^p$. We remark that the map ρ is in general not a homomorphism and that $G^{p^k} = \langle \rho^k(G)\rangle$, for any integer k. We stick to the notation from the List of Symbols.

Lemma 51. *Let p be a prime number and let G be a finite p-group. Assume that G is regular and that G_2 has exponent dividing p. Then ρ is an endomorphism of G.*

Proof. This follows directly from the definition of regularity. ∎

Lemma 52. *Let p be a prime number and let G be a finite p-group. Assume that G is regular. Then for all $k \in \mathbb{Z}_{\geq 0}$, the following hold.*

1. *One has $G^{p^k} = \rho^k(G)$.*
2. *One has $\mu_{p^k}(G) = \{x \in G \ : \ \rho^k(x) = 1\}$.*
3. *One has $|\mu_{p^k}(G)| = |G : G^{p^k}|$.*

Proof. The lemma is a combination of Satz 10.5 and Satz 10.7(a) from [Hup67], Chapter 3. ∎

We remark that p-groups satisfying conditions 1–3 from Lemma 52 are often referred to as *power abelian*.

Lemma 53. *Let p be a prime number and let G be a finite p-group. If $|G : G^p| < p^p$, then G is regular.*

Proof. The lemma is a simplified version of Satz 10.13 from [Hup67], Chapter 3. ∎

Lemma 54. *Let p be a prime number and let G be a finite regular p-group. Let M, N be normal subgroups of G and let r, s be non-negative integers. Then $[\rho^r(M), \rho^s(N)] = \rho^{r+s}([M, N])$.*

Proof. See [Hup67, Satz 10.8(a) from Ch. 3]. ∎

Lemma 55. *Assume G is a finite 3-group that can be generated by 2 elements. If G is regular, then G_2 is cyclic.*

Proof. See Satz 10.3(b) from [Hup67], Chapter 3. ∎