Commuting Probability

Thomas Browning

September 2019

For a finite group G, consider the probability

$$P(G) = \frac{|\{(g,h) \in G \times G : gh = hg\}|}{|G|^2}$$

that two elements of G commute. For example, $P(S_3) = \frac{1}{2}$, $P(D_4) = \frac{5}{8}$, $P(A_4) = \frac{1}{3}$, and $P(A_5) = \frac{1}{12}$. Clearly, $P(G) \leq 1$ with equality if and only if G is abelian. When G is nonabelian, $P(G)$ measures how far G is from being abelian. The purpose of this note is to investigate the possible values of $P(G)$.

1 The Center

For each $g \in G$, we can form the centralizer subgroup

$$C_G(g) = \{h \in G : gh = hg\}.$$

Summing over $g \in G$ gives the formula

$$P(G) = \frac{1}{|G|^2} \sum_{g \in G} |C_G(g)| . \tag{1}$$

For each $g \in G$, either $C_G(g) = G$ or $|C_G(g)| \leq \frac{1}{2}|G|$. The set of $g \in G$ for which the first possibility holds is called the center of G and is denoted by

$$Z(G) = \{g \in G : C_G(g) = G\} = \{g \in G : gh = hg \text{ for all } h \in G\}.$$

Note that $Z(G)$ is actually a normal subgroup of G. Splitting up the sum gives the estimate

$$\begin{aligned}
P(G) &= \frac{1}{|G|^2}\left(\sum_{g \in Z(G)} |C_G(g)| + \sum_{g \in G \setminus Z(G)} |C_G(g)|\right) \\
&\leq \frac{1}{|G|^2}\left(\sum_{g \in Z(G)} |G| + \sum_{g \in G \setminus Z(G)} \frac{1}{2}|G|\right) \\
&= \frac{1}{|G|^2}\left(|Z(G)| \cdot |G| + \big(|G| - |Z(G)|\big) \cdot \frac{1}{2}|G|\right) \\
&= \frac{1}{|G|}\left(|Z(G)| + \frac{1}{2}(|G| - |Z(G)|)\right) \\
&= \frac{1}{|G|}\left(\frac{1}{2}|G| + \frac{1}{2}|Z(G)|\right) \\
&= \frac{1}{2} + \frac{|Z(G)|}{2|G|}.
\end{aligned}$$

This gives the inequality

$$P(G) \leq \frac{1}{2}\left(1 + \frac{1}{[G : Z(G)]}\right) \tag{2}$$

To obtain a lower bound for $[G : Z(G)]$ for nonabelian G, we will use the fact that $G/Z(G)$ cannot be cyclic.

Lemma 1. *If $G/Z(G)$ is cyclic then G is abelian.*

Proof. Suppose that $G/Z(G)$ is generated by the coset $gZ(G)$, meaning that every element of $G/Z(G)$ is of the form $g^k Z(G)$ for some $k \in \mathbb{Z}$. Then every element of G is of the form $g^k z$ for some $k \in \mathbb{Z}$ and $z \in Z(G)$. However, any two elements of this form commute. This shows that G is abelian. $\square$

When G is nonabelian, Lemma 1 shows that $G/Z(G)$ is not cyclic. Then $[G : Z(G)] \geq 4$ so (2) gives

$$P(G) \leq \frac{1}{2}\left(1 + \frac{1}{4}\right) = \frac{5}{8}.$$

Retracing our steps shows that $P(G) = \frac{5}{8}$ if and only if $[G : Z(G)] = 4$ and $|C_G(g)| = \frac{1}{2}|G|$ for all $g \notin Z(G)$. However, the second condition is actually redundant. To see this, note that for each $g \notin Z(G)$ we have

$$Z(G) \lneq C_G(g) \lneq G.$$

In particular, if $[G : Z(G)] = 4$ then we must have $[G : C_G(g)] = 2$ for all $g \notin Z(G)$. Thus, $P(G) = \frac{5}{8}$ if and only if $[G : Z(G)] = 4$. The same argument also proves the following generalization.

Theorem 2. *Let G be a nonabelian finite group. If p is the smallest prime dividing $|G|$ then*

$$P(G) \leq \frac{p^2 + p - 1}{p^3}$$

with equality if and only if $[G : Z(G)] = p^2$.

2 The Derived Subgroup

In the previous section, we used $Z(G)$ to estimate $P(G)$. This strategy worked because $Z(G)$ provides a (rather crude) measure of how far G is from being abelian. In this section, we will instead use the derived subgroup G' to estimate $P(G)$. This will enable us to get better estimates for $P(G)$ because G' provides a more refined measure of how G is from being abelian. We first introduce the derived subgroup G' of G.

Lemma 3. $G' = \langle ghg^{-1}h^{-1} : g, h \in G \rangle$ *is the smallest normal subgroup of G with abelian quotient.*

Proof. For any $k \in G$, we have the identity

$$k(ghg^{-1}h^{-1})k^{-1} = (kgk^{-1})(khk^{-1})(kgk^{-1})^{-1}(khk^{-1})^{-1}.$$

Thus, conjugation by any $k \in G$ permutes the generators of G'. This shows that G' is a normal subgroup of G. The quotient G/G' is abelian since

$$(gG')(hG')(gG')^{-1}(hG')^{-1} = (ghg^{-1}h^{-1})G' = G'$$

for any cosets $gG', hG' \in G/G'$. If N is a normal subgroup of G with abelian quotient then for any $g, h \in G$,

$$(ghg^{-1}h^{-1})N = (gN)(hN)(gN)^{-1}(hN)^{-1} = N.$$

Thus, $ghg^{-1}h^{-1} \in N$ for any $g, h \in G$. This shows that $G' \leq N$. $\square$

The analog of (2) for G' is the inequality

$$P(G) \leq \frac{1}{4}\left(1 + \frac{3}{|G'|}\right). \tag{3}$$

A proof of this inequality is given in the appendix. When G is nonabelian, Lemma 3 shows that the derived subgroup G' is nontrivial. In particular, $|G'| \geq 2$ which recovers the estimate $P(G) \leq \frac{5}{8}$.

If $|G'| \geq 3$ then (3) gives the estimate $P(G) \leq \frac{1}{2}$. Now consider the case where $|G'| = 2$. Let $G' = \{1, x\}$. Since G' is a normal subgroup of G, we must have $gxg^{-1} = x$ for all $g \in G$. Thus, $x \in Z(G)$ which shows that $G' \leq Z(G)$. With this in mind, we now consider the case where $|G'|$ is prime and where $G' \leq Z(G)$.

2.1 Case I: $|G'| = p$ and $G' \leq Z(G)$

For each $g \in G$, consider the function $\varphi_g \colon G \to G'$ given by $\varphi_g(h) = ghg^{-1}h^{-1}$. Then since $G' \leq Z(G)$,

$$\varphi_g(h)\varphi_g(k) = (ghg^{-1}h^{-1})(gkg^{-1}k^{-1}) = ghg^{-1}(gkg^{-1}k^{-1})h^{-1} = g(hk)g^{-1}(hk)^{-1} = \varphi_g(hk)$$

for all $h, k \in G$. Thus, φ_g is a homomorphism. Also note that $\ker \varphi_g = C_G(g)$. Then by (1),

$$P(G) = \frac{1}{|G|^2}\sum_{g\in G}|C_G(g)| = \frac{1}{|G|^2}\sum_{g\in G}|\ker\varphi_g| = \frac{1}{|G|}\sum_{g\in G}\frac{1}{[G : \ker\varphi_g]} = \frac{1}{|G|}\sum_{g\in G}\frac{1}{|\operatorname{im}\varphi_g|}.$$

If $g \in Z(G)$ then $|\operatorname{im}\varphi| = 1$. Otherwise, $\operatorname{im}\varphi$ is a nontrivial subgroup of G' so $|\operatorname{im}\varphi| = p$. Thus,

$$P(G) = \frac{1}{|G|}\left(|Z(G)| + \frac{1}{p}\big(|G| - |Z(G)|\big)\right) = \frac{1}{p}\left(1 + \frac{p-1}{[G : Z(G)]}\right).$$

It remains to determine the possible values for $[G : Z(G)]$. Consider the function $\varphi \colon G \times G \to G'$ given by $\varphi(g, h) = ghg^{-1}h^{-1}$. We now prove several properties of φ.

- φ satisfies $\varphi(g, hk) = \varphi(g, h)\varphi(g, k)$ and $\varphi(gh, k) = \varphi(g, k)\varphi(h, k)$ for all $g, h, k \in G$.

  Proof. Since $G' \leq Z(G)$,

  $$\begin{aligned}\varphi(g, h)\varphi(g, k) &= (ghg^{-1}h^{-1})(gkg^{-1}k^{-1}) = ghg^{-1}(gkg^{-1}k^{-1})h^{-1} = g(hk)g^{-1}(hk)^{-1} = \varphi(g, hk),\\ \varphi(g, k)\varphi(h, k) &= (gkg^{-1}k^{-1})(hkh^{-1}k^{-1}) = g(hkh^{-1}k^{-1})kg^{-1}k^{-1} = (gh)k(gh)^{-1}k^{-1} = \varphi(gh, k),\end{aligned}$$

  as desired. □

- $\varphi(g, g) = 1$ for all $g \in G$.

  Proof. We can compute $\varphi(g, g) = ggg^{-1}g^{-1} = 1$. □

- If $g \in G$ is such that $\varphi(g, h) = 1$ for all $h \in G$ then $g \in Z(G)$.

  Proof. If $\varphi(g, h) = 1$ for all $h \in G$ then $ghg^{-1}h^{-1} = 1$ for all $h \in G$ so $g \in Z(G)$. □

If $g, h \in G$ and $z, w \in Z(G)$ then

$$\varphi(gz, hw) = \varphi(g, hw)\varphi(z, hw) = \varphi(g, h)\varphi(g, w)\varphi(z, h)\varphi(z, w) = \varphi(g, h).$$

Then we obtain a well-defined map $\overline{\varphi} \colon G/Z(G) \times G/Z(G) \to G'$. The three properties of φ that we proved give rise to three analogous properties of $\overline{\varphi}$.

- $\overline{\varphi}$ satisfies $\overline{\varphi}(x, yz) = \overline{\varphi}(x, y)\overline{\varphi}(x, z)$ and $\overline{\varphi}(xy, z) = \overline{\varphi}(x, z)\overline{\varphi}(y, z)$ for all $x, y, z \in G/Z(G)$.

- $\overline{\varphi}(x,x) = 1$ for all $x \in G/Z(G)$.
- If $x \in G/Z(G)$ is such that $\overline{\varphi}(x,y) = 1$ for all $y \in G/Z(G)$ then $x = 1$.

By the first property of $\overline{\varphi}$, we have the identity $\overline{\varphi}(x^p, y) = \overline{\varphi}(x,y)^p = 1$ for all $x, y \in G/Z(G)$. By the third property of $\overline{\varphi}$, $x^p = 1$ for all $x \in G/Z(G)$. Also note that $G/Z(G)$ is abelian by Lemma 3. This shows that $G/Z(G)$ is a vector space over $\mathbb{F}_p$, the finite field of order p. In particular, $G/Z(G)$ is an elementary abelian p-group, meaning that $G/Z(G) \cong C_p \times \cdots \times C_p$ where C_p denotes the cyclic group of order p.

The three properties of $\overline{\varphi}$ state that $\overline{\varphi}$ is a "symplectic bilinear form" on the $\mathbb{F}_p$-vector space $G/Z(G)$. As we prove in the appendix (Theorem 9), this implies that the dimension of $G/Z(G)$ over $\mathbb{F}_p$ is even. In particular, $[G : Z(G)] = p^{2n}$ for some positive integer n. We summarize this result in the following theorem.

Theorem 4. *Let G be a nonabelian finite group. If $|G'| = p$ is a prime and if $G' \leq Z(G)$ then $G/Z(G)$ is an elementary abelian p-group of order p^{2n} for some positive integer n and*

$$P(G) = \frac{1}{p}\left(1 + \frac{p-1}{p^{2n}}\right).$$

Before starting Case I, we proved that if $|G'| = 2$ then we automatically have $G' \leq Z(G)$.

Corollary 5. *Let G be a finite group.*

- *If $|G'| = 1$ then $P(G) = 1$.*
- *If $|G'| = 2$ then $P(G) = \frac{1}{2}\left(1 + 2^{-2n}\right)$ for some positive integer n.*
- *If $|G'| \geq 3$ then $P(G) \leq \frac{1}{2}$.*

We now turn our attention to the case where $|G'| = p$ and $G' \not\leq Z(G)$. In this case, $G' \cap Z(G)$ is a proper subgroup of G' so $G' \cap Z(G) = 1$ by Lagrange's theorem.

2.2 Case II: $|G'| = p$ and $G' \cap Z(G) = 1$

In this section, we will prove the following result.

Theorem 6. *Let G be a nonabelian finite group. If $|G'| = p$ is a prime and if $G' \cap Z(G) = 1$ then $G/Z(G) \cong C_p \rtimes C_k$ for some integer $k \geq 2$ dividing $p-1$ and*

$$P(G) = \frac{k^2 + p - 1}{k^2 p}.$$

Theorem 6 gives the following generalization of Corollary 5.

Corollary 7. *Let G be a finite group.*

- *If $|G'| = 1$ then $P(G) = 1$.*
- *If $|G'| = 2$ then $P(G) = \frac{1}{2}\left(1 + 2^{-2n}\right)$ for some positive integer n.*
- *If $|G'| = 3$ then either $P(G) = \frac{1}{2}$ or $P(G) = \frac{1}{3}\left(1 + 2 \cdot 3^{-2n}\right)$ for some positive integer n.*
- *If $|G'| \geq 4$ then $P(G) \leq \frac{7}{16}$.*

In particular, $P(G)$ does not takes values in the interval $(\frac{7}{16}, \frac{1}{2})$.

To prove Theorem 6, we first reduce to the case where $Z(G) = 1$. This will be done by considering the quotient $H = G/Z(G)$. If two cosets $gZ(G), hZ(G) \in H$ commute then

$$(ghg^{-1}h^{-1})Z(G) = (gZ(G))(hZ(G))(gZ(G))^{-1}(hZ(G))^{-1} = Z(G)$$

so $ghg^{-1}h^{-1} \in G' \cap Z(G) = 1$. This proves the useful result

$$(gZ(G))(hZ(G)) = (hZ(G))(gZ(G)) \iff gh = hg. \tag{4}$$

We now prove several properties of H.

- $Z(H) = 1$.

  Proof. Let $gZ(G) \in Z(H)$. By (4), $g \in Z(G)$. Then $gZ(G) = 1$ which shows that $Z(H) = 1$. $\square$

- $H' \cong G'$.

  Proof. By Lemma 3 and the third isomorphism theorem, we have $H' \leq N/Z(G)$ if and only if $G' \leq N$. Then Lemma 3 shows that $H' = (G'Z(G))/Z(G)$.

  Since G' and $Z(G)$ are normal subgroups of G with trivial intersection, the product $G'Z(G)$ is the internal direct product of G' with $Z(G)$. Then $H' = (G'Z(G))/Z(G) = (G' \times Z(G))/Z(G) \cong G'$. $\square$

- $P(H) = P(G)$.

  Proof. By (4), we can directly compute

$$\begin{aligned} P(H) &= \frac{1}{|H|^2} \left|\{gZ(G), hZ(G) \in H : (gZ(G))(hZ(G)) = (hZ(G))(gZ(G))\}\right| \\ &= \frac{|Z(G)|^2}{|G|^2} \left|\{gZ(G), hZ(G) \in G/Z(G) : gh = hg\}\right| \\ &= \frac{1}{|G|^2} \left|\{g, h \in G : gh = hg\}\right| = P(G). \end{aligned}$$ $\square$

If Theorem 6 holds for H then

$$G/Z(G) \cong H \cong H/Z(H) \cong C_p \rtimes C_k$$

for some positive $k \geq 2$ dividing $p - 1$ and

$$P(G) = P(H) = \frac{k^2 + p - 1}{k^2 p}.$$

Thus, if Theorem 6 holds for H then Theorem 6 holds for G. This allows us to reduce to the case where $Z(G) = 1$. For the remainder of this case, suppose that $Z(G) = 1$. We first show that the centralizer

$$C_G(G') = \{g \in G : gh = hg \text{ for all } h \in G'\}$$

is abelian.

Lemma 8. *If $x, y \in C_G(G')$ then $x^{-1}yxy^{-1} \in Z(G)$.*

Proof. We will use the notation $[h, k] = hkh^{-1}k^{-1}$. For each $g \in G$, we have the Hall-Witt identity

$$g[[g^{-1}, x], y]g^{-1}y[[y^{-1}, g], x]y^{-1}x[[x^{-1}, y], g]x^{-1} = 1.$$

To prove this identity, just expand it out and start cancelling terms. Since $x, y \in C_G(G')$, we have that $[[g^{-1}, x], y] = 1$ and $[[y^{-1}, g], x] = 1$. Then $[[x^{-1}, y], g] = 1$ for all $g \in G$. This shows that $[x^{-1}, y] \in Z(G)$. $\square$

Since $Z(G) = 1$, Lemma 8 shows that $C_G(G')$ is abelian. Since G' is a normal subgroup of G, we can consider the conjugation homomorphism $\varphi\colon G \to \mathrm{Aut}(G')$ where $\ker\varphi = C_G(G')$.

Recall that G' is cyclic of order p. Then a standard result in group theory states that $\mathrm{Aut}(G')$ is cyclic of order $p-1$. Applying the first isomorphism theorem to the conjugation homomorphism $\varphi\colon G \to \mathrm{Aut}(G')$ shows that $G/C_G(G')$ is cyclic of order k for some positive integer k dividing $p-1$. Let $gC_G(G')$ be a generator of $G/C_G(G')$. Then G is generated by g and $C_G(G')$.

Consider the function $f\colon C_G(G') \to G'$ given by $f(x) = gxg^{-1}x^{-1}$. Suppose that $f(x) = f(y)$ for some $x, y \in C_G(G')$. Then $gxg^{-1}x^{-1} = gyg^{-1}y^{-1}$ so $gy^{-1}x = y^{-1}xg$. In other words, $g \in C_G(y^{-1}x)$. Since $C_G(G')$ is abelian, we also have that $C_G(G') \leq C_G(y^{-1}x)$. Since G is generated by g and $C_G(G')$, we have that $C_G(y^{-1}x) = G$. Then $y^{-1}x \in Z(G)$ so $x = y$. This shows that f is injective. In particular, $|C_G(G')| \leq |G'|$. Since G' is abelian, we also have $G' \leq C_G(G')$. This shows that $C_G(G') = G'$.

To summarize, G/G' is cyclic of order k for some positive integer k dividing $p-1$. Since gG' generates G/G', g has order divisible by k. Then some power of g generates a cyclic subgroup H of order k. Since k is coprime to $p-1$, Lagrange's theorem shows that $G' \cap H = 1$. Then the recognition theorem for semidirect products shows that $G = G' \rtimes H \cong C_p \rtimes C_k$. In particular, G can be written as the disjoint union

$$G = \{1\} \cup (C_p \setminus \{1\}) \cup \underbrace{(C_k \setminus \{1\}) \cup \cdots \cup (C_k \setminus \{1\})}_{p \text{ copies}}.$$

where there is no commutation between any two of the $p+1$ nonidentity components in this decomposition. Then we can directly compute

$$P(G) = \frac{(2pk-1) + (p-1)^2 + p(k-1)^2}{p^2k^2} = \frac{k^2 + p - 1}{k^2 p}$$

where $2pk - 1$ is the number of commuting pairs involving the identity element. This proves Theorem 6.

3 Appendix: Character Theory

In this appendix, we prove (3) via character theory. We can rewrite Equation (1) as

$$P(G) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{[G : C_G(g)]}$$

where $[G : C_G(g)]$ is the size of the conjugacy class of g. Then each conjugacy class of G contributes 1 to the sum. This shows that

$$P(G) = \frac{k(G)}{|G|}$$

where $k(G)$ denotes the number of conjugacy classes of G. In other words, we would like an upper bound on the number of conjugacy classes of G. This will be done by considering the irreducible characters of G.

Let $\chi_1, \chi_2, \ldots, \chi_{k(G)}$ be the irreducible characters of G. We will need the following results:

- The number of irreducible characters of G equals the number of conjugacy classes of G.
- Each irreducible character χ_i of G has a degree $\deg\chi_i$ which is a positive integer.
- $\sum_i (\deg\chi_i)^2 = |G|$.
- The number of irreducible characters of G of degree 1 equals $[G : G']$.

We can make the estimate

$$|G| = \sum_{i=1}^{k(G)} (\deg\chi_i)^2 \geq [G : G'] + 4(k(G) - [G : G']) = 4k(G) - 3\frac{|G|}{|G'|}.$$

Then dividing through by $4\,|G|$ and rearranging terms shows that

$$P(G) = \frac{k(G)}{|G|} \leq \frac{1}{4}\left(1 + \frac{3}{|G'|}\right)$$

as desired.

4 Appendix: Symplectic Vector Spaces

Let F be a field and let V be a finite-dimensional vector space over F. A symplectic bilinear form on V is a function $\omega\colon V \times V \to F$ that satisfies:

- $\omega(x, y + z) = \omega(x, y) + \omega(x, z)$ and $\omega(x + y, z) = \omega(x, z) + \omega(y, z)$ for all $x, y, z \in V$.
- $\omega(cx, y) = c\omega(x, y)$ and $\omega(x, cy) = c\omega(x, y)$ for all $x, y \in V$ and $c \in F$.
- $\omega(x, x) = 0$ for all $x \in V$.
- If $x \in V$ is such that $\omega(x, y) = 0$ for all $y \in V$ then $x = 0$.

Suppose that there exists a symplectic bilinear form ω on V. Then for all $x, y \in V$, we have the identity

$$0 = \omega(x + y, x + y) = \omega(x, x) + \omega(x, y) + \omega(y, x) + \omega(y, y) = \omega(x, y) + \omega(y, x).$$

This shows that $\omega(x, y) = -\omega(y, x)$ for all $x, y \in V$. Now suppose that $\dim V \geq 1$. Let $x \in V \setminus \{0\}$. Then there exists a $y \in V$ such that $\omega(x, y) \neq 0$. Note that $\omega(x, cx) = c\omega(x, x) = 0$ for all $c \in F$. Then $y \notin \langle x \rangle$ which shows that $\dim\langle x, y \rangle = 2$. Let

$$W = \{z \in V : \omega(x, z) = \omega(y, z) = 0\}.$$

We now prove several properties of W.

- $\dim W \geq \dim V - 2$.

  Proof. Note that $W = \ker \varphi$ where $\varphi\colon V \to F^2$ is the linear transformation given by

  $$\varphi(z) = (\omega(x, z), \omega(y, z)).$$

  Then $\operatorname{rank} \varphi \leq 2$ so

  $$\dim W = \dim \ker \varphi = \dim V - \operatorname{rank} \varphi \geq \dim V - 2$$

  by the rank-nullity theorem. □

- $V = \langle x, y \rangle \oplus W$.

  Proof. Let $z \in \langle x, y \rangle \cap W$. Then $z = cx + dy$ for some $c, d \in F$. We have the identities

  $$\begin{aligned} 0 = \omega(x, z) &= \omega(x, cx + dy) = c\omega(x, x) + d\omega(x, y) = d\omega(x, y), \\ 0 = \omega(x, z) &= \omega(y, cx + dy) = c\omega(y, x) + d\omega(y, y) = -c\omega(x, y). \end{aligned}$$

  Then $c = d = 0$ since $\omega(x, y) \neq 0$. This shows that $\langle x, y \rangle \cap W = \{0\}$. Then the previous property shows that $V = \langle x, y \rangle \oplus W$. □

- There exists a symplectic bilinear form $\widetilde{\omega}$ on W.

Proof. Let $\widetilde{\omega}\colon W \times W \to F$ be given by $\widetilde{\omega}(x, y) = \omega(x, y)$ for all $x, y \in W$. In other words, $\widetilde{\omega}$ is just the restriction of ω to W. Since ω satisfies the first three axioms of a symplectic bilinear form, so does $\widetilde{\omega}$. It remains to show that $\widetilde{\omega}$ satisfies the fourth axioms of a symplectic bilinear form. Let $w \in W$ be such that $\widetilde{\omega}(w, z) = 0$ for all $z \in W$. Then $\omega(w, z) = 0$ for all $z \in W$. We also know that $\omega(w, x) = 0$ and $\omega(w, y) = 0$. By linearity, $\omega(w, z) = 0$ for all $z \in \langle W, x, y \rangle = V$. □

In summary, we have shown that if $\dim V \geq 1$ then there exists a subspace W of V with $\dim W = \dim V - 2$ and there exists a symplectic bilinear form on W. Then induction on $\dim V$ proves the following theorem.

Theorem 9. *Let V be a finite dimensional vector space over a field F. Suppose that there exists a symplectic bilinear form ω on V. Then $\dim V$ is even.*