Consider the following setup: let $G$ be an algebraic group over some field $k$. What can we say about finite subgroups of $G$? In particular, is it possible to bound above the orders of such subgroups?

The history of such a question goes a long way back, starting from Minkowski, then Schur and others. We will briefly introduce some weak bounds given by Minkowski, then proceed to give bounds which are closely related to Schur’s idea. These bounds are not optimal for a general $G$, but are ‘very close’ to being such, and much easier to deal with than an optimal bound.

We start by introducing some notation. Let $l$ be a prime, and $v_l$ the standard $l$-valuation on the $l$-adic numbers $\mathbb{Q}_l$. We will also write $v_l(A)$ to denote $v_l(|A|)$, if $A$ is a finite set. Unless specified differently, $k$ will be a field of characteristic different from $l$.

1 The beginning: Minkowski bounds for $GL_n$

The story of our topic starts at the beginning of the 20th century, when Minkowski proves

**Theorem 1.** Let $n \geq 1$, define

$$M(n,l) = \left\lfloor \frac{n}{l-1} \right\rfloor + \left\lfloor \frac{n}{l(l-1)} \right\rfloor + \left\lfloor \frac{n}{l^2(l-1)} \right\rfloor + \ldots$$

Suppose $A \subset GL_n(\mathbb{Q})$ is a finite subgroup, then $v_l(A) \leq M(n,l)$. Moreover this bound is sharp, that is, there exists a finite $l$-subgroup $A \subset GL_n(\mathbb{Q})$ with $v_l(A) = M(n,l)$.

*Proof.* See [4] for the details, let’s sketch the proof of the first claim.

**Lemma 2.** If $m \geq 3$, the kernel of

$$GL_n(\mathbb{Z}) \longrightarrow GL_n(\mathbb{Z}/m\mathbb{Z})$$

if torsion free.

This is an easy exercise, or an easy consequence of results in formal groups over local rings. First of all, notice that $A$ is conjugate to a subgroup of $GL_n(\mathbb{Z})$, because this is equivalent to finding an $A$-stable lattice in $\mathbb{Q}^n$, and one such is the lattice generated by $A$-translations of $\mathbb{Z}^n$. Thus, we can assume $A \subset GL_n(\mathbb{Z})$.

Similarly, we can find a positive definite quadratic form on $\mathbb{Q}^n$ with integral coefficients that is $A$-invariant, just sum the $A$-translates of $\sum_i x_i^2$. 


Suppose now \( l > 2 \), the case \( l = 2 \) is slightly more complicated. Take \( p \) an odd prime number, by the lemma \( A \rightarrow \text{GL}_n(\mathbb{Z}/p\mathbb{Z}) \) is an injective map, hence
\[
v_l(A) \leq a(p) := v_l(\text{GL}_n(\mathbb{Z}/p\mathbb{Z})) = \sum_{i=1}^{n} v_l(p^i - 1).
\]
Take now \( p \) so that \( a(p) \) is as small as possible, which corresponds to \( p \) being a generator of \((\mathbb{Z}/l^2\mathbb{Z})^*\), and one such exists by Dirichlet’s theorem on arithmetic progressions.

We have moreover \( v_l(p^i - 1 - 1) = 1 \) and \( v_l(p^i - 1) = 1 + v_l(i) \) if \( (l - 1)|i \), then we compute \( a(p) \) and find that it is equal to the RHS of the claim of the theorem.

**Remark.** It is not too hard to generalize by taking a number field instead than \( \mathbb{Q} \) and proving similar statements.

### 2 Invariants

We will determine bounds in terms of certain invariants depending on the field \( k \) and the prime \( l \).

We define these invariants in this section.

For every natural number \( n \) coprime with \( \text{char} k \), the group of \( n \)-th roots of unity
\[
\mu_n = \langle \xi_n \rangle
\]
is contained in the separable closure \( k_s \) and the absolute Galois group \( \Gamma_k = \text{Gal}(k_s|k) \) acts on \( \mu_n \), giving in fact a continuous morphism
\[
\chi_n : \Gamma_k \rightarrow \text{Aut}(\mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^* \text{ called the } n\text{-th cyclotomic character .}
\]
As \( n \) varies among the powers of \( l \), we can take the inverse limit and get the \( l^\infty \)-cyclotomic character
\[
\chi_{l^\infty} : \Gamma_k \rightarrow \mathbb{Z}_l^* = \varprojlim (\mathbb{Z}/l^d\mathbb{Z})^*,
\]
we are in particular interested in the closed subgroup \( \text{Im}\chi_{l^\infty} \subset \mathbb{Z}_l^* \).

#### 2.1 The case \( l \neq 2 \)

We have
\[
\mathbb{Z}_l^* = C_{l-1} \times \{1 + l \cdot \mathbb{Z}_l\}
\]
where \( C_{l-1} \cong \mathbb{F}_l^* \) is cyclic of order \( l - 1 \) while \( \{1 + l^d \mathbb{Z}_l\} \cong \mathbb{Z}_l \) has as closed subgroups \( \{1 + l^d \mathbb{Z}_l\} = \langle 1 + l^d \rangle \) for every \( d = 1, 2, \ldots, \infty \). Any closed subgroup of \( \mathbb{Z}_l^* \) decomposes as a direct product since \( (l - 1, l) = 1 \), thus
\[
\text{Im}\chi_{l^\infty} = C_l \times \{1 + l^m \mathbb{Z}_l\}
\]
for some cyclic subgroup \( C_l \subset C_{l-1} \) and some \( m \in \{1, \ldots, \infty\} \).

An easier way to describe the invariants \( t \) and \( m \) is:
\[
t = [k(\xi_l) : k]
\]
\[
m = \text{upper bound of } d \geq 1 \text{ such that } \xi_{ld} \in k(\xi_l).
\]

**Example 1.** When \( k = \mathbb{Q} \), we have \( t = l - 1 \) and \( m = 1 \), so in fact \( \chi_{l^\infty} \) is surjective.
2.2 The case \( l = 2 \)

Now
\[
Z_2^* = C_2 \times \{1 + 4 \cdot Z_2\}
\]
and we have three possibilities for \( \text{Im} \chi \ell \infty \):

A. \( \text{Im} \chi \ell \infty = 1 + 2^m \cdot Z_2 = \langle 1 + 2^m \rangle \) for \( m \geq 2 \), we set \( t = 1 \);

B. \( \text{Im} \chi \ell \infty = \langle -1 + 2^m \rangle \) for \( m \geq 2 \), we set \( t = 2 \);

C. \( \text{Im} \chi \ell \infty = C_2 \times \{1 + 2^m \cdot Z_2\} = \langle -1, 1 + 2^m \rangle \) for \( m \geq 2 \), we set \( t = 2 \).

Again, we have an alternative description which is somewhat more complicated. We have
\[
t = [k(z_4) : k] = [k(i) : k]
\]
but the description of \( m \) depends on the case:

\[
m = \begin{cases} 
-1 + \text{upper bound of } d \geq 1 \text{ such that } \xi_{2d} \in k(i) & \text{in case (b)} \\
\text{upper bound of } d \geq 1 \text{ such that } \xi_{2d} \in k(i) & \text{otherwise}
\end{cases}
\]

**Example 2.** If \( k = \mathbb{Q} \), we have case (c) with \( t = 2 \) and \( m = 2 \).

2.3 Finiteness of the invariants

Clearly \( t \) is always finite, but how about \( m \)? It is evident by the definition that \( m = \infty \) if and only if \( \text{Im} \chi \ell \infty \) is a finite subgroup.

**Proposition 3.** Let \( k_0 \) be the prime subfield of \( k \). If \( k \) is finitely generated over \( k_0 \) then \( m \) is finite.

**Proof.** Arguing by contradiction, suppose \( m = \infty \), that is \( \text{Im} \chi \ell \infty \) is finite. Then there is a finite extension \( k' \supset k \) given by Galois correspondence which is a fixed field for every automorphism of \( \mu_{t^d} \) for every \( d \geq 1 \), hence \( k' \) contains the group \( \mu \) of all the \( t^d \)-th roots of unity. Let \( K = k_0(\mu) \), clearly \( K \supset k_0 \) is an algebraic extension, and \( K \) is finitely generated over \( k_0 \), because \( k' \) is, as it is a finite extension of a finitely generated extension. Now if \( k_0 = \mathbb{Q} \) then \( K \) must be a number field, while if \( k_0 = \mathbb{F}_p \) then \( K \) is a finite field. In both cases we have a contradiction as no such \( K \) contains infinitely many roots of unity. \( \square \)

3 Bounds for tori

**Theorem 4.** Let \( T \) be an \( n \)-dimensional \( k \)-torus, \( A \) a finite subgroup of \( T(k) \). Then
\[
v_t(A) \leq m \cdot \left\lfloor \frac{n}{\phi(t)} \right\rfloor
\]
where the invariants \( t \) and \( m \) are defined as above, and \( \phi \) is Euler’s function.

In fact, this bound is optimal:
Theorem 5. Suppose \( m < \infty \). Then for every \( n \geq 1 \) there exists a \( k \)-torus \( T \) of dimension \( n \) and a finite subgroup \( A \subset T(k) \) such that

\[
v_l(A) = m \cdot \left\lfloor \frac{n}{\phi(t)} \right\rfloor
\]

In this section we prove both theorems.

Lemma 6. Let \( u \in \text{Mat}_n(\mathbb{Z}_l) \), and consider \( u \) as an endomorphism of \( (\mathbb{Q}_l/\mathbb{Z}_l)^n \). Then

\[
v_l(\ker u) = v_l(\det u).
\]

Proof. The claim is obvious if \( u = \text{diag}(\lambda_i) \) is a diagonal matrix, because the kernel of the multiplication by \( \lambda_i \in \mathbb{Z}_l \) on \( \mathbb{Q}_l/\mathbb{Z}_l \) is exactly \( \lambda_i^{-1}\mathbb{Z}_l/\mathbb{Z}_l \) which has cardinality \( v_l(\lambda_i) \).

If \( u \) is not diagonal, we can multiply on the left and on the right by matrices \( A, B \in \text{GL}_n(\mathbb{Z}_l) \) and put it in diagonal form. These matrices are invertible, hence \( |\ker u| = \ker(AuB) \) and their determinant is in \( \mathbb{Z}_l^* \), thus \( v_l(\det(AuB)) = v_l(\det A) + v_l(\det u) + v_l(\det B) = v_l(\det u). \)

Denote now \( \chi = \chi_{l^\infty} \). Let \( Y(T) = \text{Hom}_{k_s}(\mathbb{G}_m, T) \) be the cocharacters group with the induced \( \Gamma_k \)-action giving a map

\[
\rho : \Gamma_k \longrightarrow \text{Aut}(Y(T)) \cong \text{GL}_n(\mathbb{Z}).
\]

Choose a basis of \( Y(T) \) which then gives a \( k_s \)-splitting

\[
T \cong \mathbb{G}_m \times \ldots \times \mathbb{G}_m \quad \text{over } k_s:
\]

in this isomorphism the \( l \)-torsion points of \( T(k_s) \) (that is, every point that has order a power of \( l \)) form a group isomorphic to \( (\mathbb{Q}_l/\mathbb{Z}_l)^n \), and the action of \( g \in \Gamma_k \) is like \( \rho(g)\chi(g) \).

Lemma 7. For every \( g \in \Gamma_k \) we have

\[
v_l(A) \leq v_l(\det(\rho(g)\chi(g) - 1)) = v_l(\det(\rho(g^{-1}) - \chi(g))).
\]

Proof. Replace \( A \) with its \( l \)-Sylow if necessary, so that \( A \) can be assumed to be an \( l \)-group and is hence contained in the subgroup of the \( l \)-torsion points of \( T(k_s) \). As \( A \subset T(k) \) is made of rational points, it is fixed by every \( g \in \Gamma_k \) acting on the \( l \)-torsion points, and hence \( A \subset \ker(g - 1) \).

Thus \( v_l(A) \leq v_l(\ker(g - 1)) = v_l(\ker(\rho(g)\chi(g) - 1)) = v_l(\det(\rho(g)\chi(g) - 1)) \)

by the previous lemma. To get the second equality, notice that

\[
\rho(g)\chi(g) - 1 = \rho(g)\chi(g) - \rho(g)\rho(g^{-1}) = -\rho(g) \cdot (\rho(g^{-1}) - \chi(g))
\]

but now \( \rho(g) \in \text{Aut}(Y(T)) \cong \text{GL}_n(\mathbb{Z}) \) hence \( \det(\rho(g)) \) has zero \( l \)-valuation, thus

\[
v_l(\det(\rho(g)\chi(g) - 1)) = v_l(\det(\rho(g)) \cdot \det(\rho(g^{-1}) - \chi(g)))
\]

\[
= v_l(\det(\rho(g)) + v_l(\det(\rho(g^{-1}) - \chi(g))) = v_l(\det(\rho(g^{-1}) - \chi(g))).
\]

All it remains to do in order to prove the first theorem of this section is to pick a \( g \in \Gamma_k \) which gives the right bound. Take a \( g \in \Gamma_k \) such that

\[
\chi(g) = \xi_tu \quad \text{where } \xi_t \in \mathbb{Z}_l^* \text{ has order } t \text{ and } v_l(1 - u) = m.
\]
Notice that such a $g$ exists by the definitions of the invariants $t$ and $m$ in relation with $\text{Im} \chi$.

We now have that $\rho(g) \in \text{GL}_n(\mathbb{Z})$ is an element of finite order, because the image of $\rho : \Gamma_k \rightarrow \text{GL}_n(\mathbb{Z})$ is finite, hence the characteristic polynomial $F$ of $\rho(g^{-1})$ is a product of cyclotomic polynomials

$$F = \prod \Phi_{d_j} \quad \text{where} \quad \sum \phi(d_j) = \deg F = n.$$ 

By the previous lemma we get

$$v_l(A) \leq v_l(\det(\rho(g^{-1}) - \chi(g))) = v_l(F(\chi(g))) = v_l\left(\prod \Phi_{d_j}(\chi(g))\right) = \sum v_l(\Phi_{d_j}(\xi u))$$

The following lemma calculates the evaluations that we need.

**Lemma 8.** We have

$$v_l(\Phi_{d}(\xi u)) = \begin{cases} m & \text{if } d = t \\ 1 & \text{if } d = tl^\alpha, \alpha \geq 1 \text{ or } \alpha = -1 \text{ in case } t = 2 = l \\ 0 & \text{otherwise} \end{cases}$$

**Proof.** Calculations. Consider the cyclotomic polynomials over $\overline{\mathbb{Q}}_l$ and split the various cases. □

We can finally prove theorem 4.

Denote by $c_1$ the number of $j$'s with $d_j = t$ as in lemma 8 and by $c_2$ the number of $j$'s with $d_j = tl^{\alpha_j}$ with $\alpha_j$ respecting the conditions of the same lemma. Using the previous lemmas we get

$$v_l(A) \leq \sum v_l(\Phi_{d_j}(\xi u)) = c_1m + c_2$$

but clearly

$$\dim T = n = \deg F = \sum \deg \Phi_{d_j} = \sum \phi(d_j) \geq c_1 \phi(d_t) + \sum_{d_j = tl^{\alpha_j}} \phi(tl^{\alpha_j}).$$

Now $\phi(tl^{\alpha_j}) \geq \phi(t)(l-1)$ hence

$$n \geq c_1 \phi(t) + c_2 \phi(t)(l-1)$$

hence

$$c_1 + c_2 (l-1) \leq \left\lfloor \frac{n}{\phi(t)} \right\rfloor$$

and concluding

$$v_l(A) \leq c_1m + c_2 \leq c_1m + c_2(l-1)m \leq m \cdot \left\lfloor \frac{n}{\phi(t)} \right\rfloor,$$

because $(l-1)m$ is a positive integer.

To show that this bound is optimal (on any field $k$) as theorem 5 states, it is enough to construct a $k$-torus $T$ of dimension $n = \phi(t)$ with a cyclic subgroup of order $l^m$ inside the rational points $T(k)$.

Let then

$$K = \begin{cases} k(\xi) & \text{if } l \neq 2 \\ k(i) & \text{if } l = 2 \end{cases}$$
this is a cyclic extension of \( k \) of degree \( t \) (by definition of the invariant \( t \)) and Galois group \( C_t \). Take the Weyl restriction \( T_1 = R_{K/k} G_m \) so that \( T_1(k) = K^* \) contains the group \( \langle \xi^m \rangle \), by definition of the invariant \( m \). Let \( \sigma \) be a generator of \( C_t \); it acts on \( T_1 \) and we have

\[
\sigma^t - 1 = 0 \in \text{End}(T_1),
\]

writing \( X^t - 1 = \Phi_t(X) \cdot G(X) \) where \( \Phi_t \) is the \( t \)-th cyclotomic polynomial, we have that

\[
\Phi_t(\sigma)G(\sigma) = 0 \in \text{End}(T_1).
\]

Pick then

\[
T = \text{Im} (G(\sigma) : T_1 \to T_1),
\]

one checks that \( \dim T = \phi(t) \) and that \( T(k) \) still contains \( \langle \xi^m \rangle \), so we found the required torus.

4 Bounds for reductive groups

Let now \( G \) be a linear algebraic group, smooth over a field \( k \). We assume \( G \) is reductive, that is, connected and with trivial unipotent radical.

We need the following introductory result.

**Theorem 9.** Let \( A \) be a finite nilpotent group of order prime to \( \text{char} \ k \) acting by \( k \)-automorphisms on \( G \). Then there exists a maximal torus \( T \) of \( G \), defined over \( k \), which is \( A \)-stable.

This is quite an important result, so we’ll sketch a step-by-step proof.

**Proposition 10.** Let \( s : G \to G \) a surjective homomorphism and assume \( k \) is algebraically closed. Then there exists a borel subgroup \( B \subset G \) such that \( s(B) = B \).

**Proof.** This follows from the following

**Fact 11.** Let \( G \) be a connected linear algebraic group over \( k = \bar{k} \), \( \sigma : G \to G \) a surjective homomorphism, and \( B \) a Borel subgroup fixed by \( \sigma \). Then the map

\[
\alpha : G \times B \to G \quad (x, b) \mapsto xb\sigma(x)^{-1}
\]

is surjective.

for whose proof see [3].

Let then \( B \) be a Borel subgroup of \( G \), then \( s(B) \) is also a Borel subgroup so that \( yBx^{-1} = B \) for some \( y \in G \) as the Borel are all conjugate. Applying the fact to the surjective homomorphism \( c_y \circ s \) we have

\[
y^{-1} = xb(c_y \circ s)(x)^{-1} = xb(ys(x)y^{-1})^{-1} = bys(x)^{-1}y^{-1}
\]

for some \( x \in G, b \in B \).

Hence

\[
y = b^{-1}x^{-1}s(x)
\]

thus

\[
B = yBx^{-1} = b^{-1}x^{-1}s(x)s(B)s(x)^{-1}xb
\]

which implies

\[
B = x^{-1}s(xBx^{-1})x \Rightarrow xBx^{-1} = s(xBx^{-1})
\]

and we found a Borel fixed by \( s \). 

\( \square \)
We’re now ready to start the proof of the theorem, which goes by induction on $|A| + \dim G$. Clearly if $G$ is a torus, we just pick $T = G$. If $|A| = 1$ just pick any maximal $k$-torus $T \subset G$, there is at least one by Grothendieck’s theorem.

Assume now $|A| > 1$. Then, being nilpotent, $A$ contains a cyclic normal subgroup $A' = \langle s \rangle$. We can assume that $G$ is semisimple and $A$ acts faithfully, or otherwise consider the action

$$A/\ker \rho \rightarrow G/R(G)$$

where $\rho : A \rightarrow G$ was the original action and $R(G)$ is the radical of $G$, which factors through the action as $A$ is nilpotent and finite.

Let $G^s$ be the $k$-subgroup fixed by $s$ and $G_1 = (G^s)^0$ its identity component, then $\dim G_1 > 0$: this can be checked geometrically and an easy application of the previous proposition shows that when $k = \overline{k}$ and $(ord(s), \text{char} k) = 1$, there is a Borel $B$ and torus $T \subset B$ such that $s(B) = B$ and $s(T) = T$. But then such a pair $(B, T)$ determines canonically a homomorphism

$$h : \mathbb{G}_m \rightarrow T$$

as $B$ gives a basis of the root system of $(G, T)$ and we take $h$ as two times the sum of the coroots. Clearly as $G$ is not a torus, $h$ is non-trivial and its canonicity implies that it is fixed by $s$, thus $G^s \supset \text{Im}(h) = S^1$.

Now $A/A'$ acts on $G_1$ and by induction there’s a maximal torus $T_1$ of $G_1$, defined over $k$, stable $A/A'$ and hence under $A$. Let $G_2 = Z_G(T_1)$ which is again reductive and has the same rank as $G$ but $\dim G_2 < \dim G$ as $T_1$ is not central in $G$. As $T$ is $A$-stable, so is $G_2$ so by the induction hypothesis applied to the pair $(G_2, A)$ we get a maximal $k$-torus $T$ of $G_2$ which is $A$-stable. Since $G_2$ and $G$ have the same rank, $T$ is also a $k$-torus for $G$. This concludes the proof of the theorem.

**Corollary 12.** Let $A \subset G(k)$ be a finite nilpotent group of order prime to $\text{char} k$. Then there is a maximal $k$-torus $T \subset G$ whose normalizer $N$ is such that $A \subset N(k)$.

**Proof.** Apply the theorem using the conjugation action.

The following bound is usually quite strict, even if not sharp.

**Theorem 13.** Let $G$ have rank $r$, with Weyl group $W$. If $A \subset G(k)$ is a finite subgroup then

$$v_l(A) \leq m \left\lfloor \frac{r}{\phi(t)} \right\rfloor + v_l(W)$$

**Proof.** As in the case of tori, we can assume that $A$ is an $l$-group, in particular it is nilpotent so by corollary 12 there is a maximal $k$-torus $T \subset G$ whose normalizer $N = N_G(T)$ is such that $A \subset N(k)$. Setting $W_T = N/T$ we get a finite $k$-group such that $W_T(k_s) \cong W$. Denote $A_T = A \cap T(k)$, we get an exact sequence

$$1 \rightarrow A_T \rightarrow A \xrightarrow{\pi} W_T(k)$$

where $\pi : A \rightarrow N(k) \rightarrow W_T(k)$ is the composition. Thus

$$v_l(A) \leq v_l(A_T) + v_l(W_T(k)).$$

Now $A_T \subset T(k)$, so we can apply theorem 4 and get

$$v_l(A_T) \leq m \cdot \left\lfloor \frac{r}{\phi(t)} \right\rfloor$$

while $W_T(k)$ is isomorphic to a subgroup of $W \cong W_T(k_s)$, hence $v_l(W_T(k)) \leq v_l(W)$ and the theorem follows.
Corollary 14. Suppose $r < \phi(t)$ where $t$ is the invariant defined before. Then $G(k)$ is $l$-torsion free, that is, it does not admit any element of order $l$.

Proof. As $\left\lfloor \frac{r}{\phi(t)} \right\rfloor = 0$, by the previous theorem it is sufficient to show that $v_l(W) = 0$. This follows from the Minkowski bound, because the Weyl group $W$ is (isomorphic to) a subgroup of $\text{GL}_r(\mathbb{Z})$ and $r < \phi(t) \leq t \leq l - 1$ hence

$$v_l(W) \leq M(r,l) = \left\lfloor \frac{r}{l-1} \right\rfloor + \left\lfloor \frac{r}{l(l-1)} \right\rfloor + \left\lfloor \frac{r}{l^2(l-1)} \right\rfloor + \ldots = 0.$$

Remark. It may look like this bound is somehow coarse, as the torus $T$ in the proof is not any torus of dimension $r$, but a subtorus of $G$, so the bound for the tori may not be attained by $T$. Moreover, the Weyl group $W_T(k)$ could be much smaller than $W$. But in fact surprisingly it is quite a precise bound.

References


