On prime numbers in orders of number fields and some applications

Boris Širola
University of Zagreb

Representation Theory XIX

(Dubrovnik, June 27, 2025.)

Plan of the talk

Plan of the talk:

1. Notation, some (well known) definitions and our setting
2. Results on primes in orders of number fields
3. Some applications:
   - (3.1) Reducibility of polynomials
   - (3.2) On "generalized modular groups" and Frattini subgroups

Notation

A integral domain, $\quad A^\times = A \setminus \{0\}$,

A^* = group of invertible elements

$\mathrm{Pr}\, A$ = set of prime elements in A

$\mathrm{Irr}\, A$ = set of irreducible elements in A

Def. $x, y \in A$ are *associated*, $x \sim y$, if $x = uy$ for some unit u.

Define $\widehat{\mathrm{Pr}}\, A = \mathrm{Pr}\, A / \sim$, the set of equivalence classes

Remark.

(1) We have $\mathrm{Pr}\, A \subseteq \mathrm{Irr}\, A$.

(2) If A is a factorization domain (e.g., A Noetherian), then:

$$A \text{ is a UFD} \quad \Leftrightarrow \quad \mathrm{Pr}\, A = \mathrm{Irr}\, A.$$

(3) In general it is more difficult to understand $\widehat{\mathrm{Pr}}\, A$ than $\widehat{\mathrm{Irr}}\, A$.

Orders in number fields

$\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{C}$, number field

$\mathcal{O} = \mathcal{O}_{\mathbb{K}}$ the ring of integers

Remark.

(1) $\mathcal{O}$ is a Dedekind domain ($\mathcal{O}$ Noetherian, integrally closed in $\mathbb{K}$ and every prime ideal $(0) \neq P$ is maximal).

(2) A Dedekind domain is a UFD iff it is a PID. In particular:

$$\mathcal{O} \text{ is a PID} \quad \Leftrightarrow \quad \mathcal{O} \text{ is a UFD} \quad \Leftrightarrow \quad \text{class number } h_{\mathbb{K}} = 1$$

Def. A subring $R \leq \mathcal{O}$ is an *order* in $\mathbb{K}$ if the index $(\mathcal{O} : R)$ (of additive groups) is finite.

Example. If $d \equiv 2, 3 \pmod 4$ is square-free, then every order in $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ is of the form

$$R_m = \{x + my\sqrt{d} \mid x, y \in \mathbb{Z}\}, \quad m \in \mathbb{N}.$$

If $d \equiv 1 \pmod 4$ is square-free, then every order in $\mathbb{K}$ is of the form

$$R_m = \{x + my\omega \mid x, y \in \mathbb{Z}\}, \quad m \in \mathbb{N};$$

where $\omega = (1 + \sqrt{d})/2$.

Fact. If $R \neq \mathcal{O}$, then R is not a UFD, and then we have a strict inclusion $\operatorname{Pr} R \subset \operatorname{Irr} R$.

Problem. Given an order R in $\mathbb{K}$, to understand the sets $\widehat{\operatorname{Pr}} R$ (and $\operatorname{Pr} R$). Find as much as possible concrete "nice" primes in R.

2. Results on primes in orders

Given any finite field extension $\mathbb{K}|\mathbb{F}$, for any $x \in \mathbb{K}$ define an $\mathbb{F}$-linear map $f_x : \mathbb{K} \to \mathbb{K}$, $f_x(y) = xy$. Define the *norm map*

$$N = N_{\mathbb{K}|\mathbb{F}} : \mathbb{K} \to \mathbb{F}, \qquad N(x) = \det f_x.$$

Remark.
(1) $N(xy) = N(x)N(y), \quad \forall x, y \in \mathbb{K}.$

(2) For a number field $\mathbb{K}|\mathbb{Q}$, $N(\mathcal{O}) \subseteq \mathbb{Z}$; i.e., we have the norm $N : \mathcal{O} \to \mathbb{Z}$.

- Some results

Thm. 1. *Let $\mathbb{K}$ be a number field. Suppose R is an order in $\mathbb{K}$ and $p \in R$ is an element s.t. $|N(p)| = \pi$, for some prime number $\pi \in \mathbb{N}$. Then $p \in \Pr R$.*
(If $\rho \in R$ is s.t. $|N(\rho)| = m$, where m is a composite number not of the form $m = \pi^k$ for some prime number $\pi \in \mathbb{N}$ and $k > 1$, then $\rho \notin \Pr R$.)

Remark. We can have some prime number $\pi \in \mathbb{N}$ and $p_1, p_2 \in R$ primes s.t. $|N(p_1)| = \pi = |N(p_2)|$ and p_1 and p_2 are *not* associated (e.g., $\mathbb{K} = \mathbb{Q}(\sqrt{10})$, $\pi = 31$, $p_1 = 11 + 3\sqrt{10}$, $p_1 = 29 + 9\sqrt{10}$).

Ancient fact. The set $\widehat{\mathrm{Pr}}\,\mathbb{Z}$ is infinite.

Question. Given a number field $\mathbb{K}$ and an order R in it, is the set $\widehat{\mathrm{Pr}}\,R$ necessarily infinite? (Note that in particular for $R = \mathcal{O}$ the group $\mathcal{O}^*$ is almost always infinite.)

Cor. *Let $d > 1$ be a square-free positive integer and R be an order in $\mathbb{K} = \mathbb{Q}(\sqrt{d})$. Then $\widehat{\mathrm{Pr}}\,R$ is infinite.*

Recall: Assume $A \subseteq B$ is an integral extension of integral domains.

• If $\mathfrak{p} \in \operatorname{Spec} A$, then there is $\mathfrak{q} \in \operatorname{Spec} B$ s.t. $\mathfrak{q} \cap A = \mathfrak{p}$; i.e., $\mathfrak{q}$ is over $\mathfrak{p}$.

Fact. (1) A fiber $\mathcal{F}_{\mathfrak{p}} = \{\mathfrak{q} \in \operatorname{Spec} B \mid \mathfrak{q} \text{ is over } \mathfrak{p}\}$ is nonempty and finite.

(2) Suppose B is a PID. Suppose $\mathfrak{q}_1, \mathfrak{q}_2 \in \mathcal{F}_{\mathfrak{p}}$ and let $\mathfrak{q}_j = (\gamma_j)$ for some $\gamma_j \in B$. Then

$$\mathfrak{q}_1 = \mathfrak{q}_2 \quad \Longleftrightarrow \quad \gamma_1 \sim \gamma_2 \quad (\gamma_j \in \operatorname{Pr} B)$$

Therefore if $\mathcal{O}$ is a PID, then $\widehat{\operatorname{Pr}}\,\mathcal{O}$ is infinite.

The following is a direct proof of "constructive flavor".

Thm. 2. *Let $\mathbb{K}$ be a number field s.t. its ring of integers $\mathcal{O}$ is a PID. Then the set $\widehat{\Pr}\,\mathcal{O}$ is infinite. (Note that $\Pr\mathcal{O} = \mathcal{O}^*\ \widehat{\Pr}\,\mathcal{O}$.)*

Sketch of the proof.
Let $[\mathbb{K} : \mathbb{Q}] = k$ and $\pi \in \mathbb{N}$ is any prime number.

If there is $p \in \mathcal{O}$ s.t. $|N(p)| = \pi$, then $p \in \Pr\mathcal{O}$. (Thm. 1)

Now suppose there is no $a \in \mathcal{O}$ s.t. $|N(a)| = \pi$, and let then $m \in \mathbb{N}$ be s.t. for any $1 \leq \ell \leq m$ there is no a satisfying $|N(a)| = \pi^\ell$ but we can find some a s.t. $|N(a)| = \pi^{m+1}$.

(Such m exists and $m < k$.)

Next suppose that $\pi \notin \Pr\mathcal{O}$ (i.e., π is not inert). Then $\exists x^{(1)}, y^{(1)} \in \mathcal{O}^\times \setminus \mathcal{O}^*$ s.t.

$$\pi = x^{(1)}y^{(1)} \quad \Rightarrow \quad \pi^k = N(x^{(1)})N(y^{(1)}).$$

We can assume: $|N(x^{(1)})| = \pi^r$, where $r \leq \lceil \frac{k}{2} \rceil$ (and $r > m$).

If $x^{(1)} \in \Pr \mathcal{O}$ we are done. If not, write $x^{(1)} = x^{(2)} y^{(2)}$ and proceed by inductive argument...

This procedure for any prime $\pi \in \mathbb{N}$ gives at least one prime $p(\pi) \in \Pr \mathcal{O}$ s.t. $|N(p(\pi))| = \pi^{\lambda(\pi)}$, for some $\lambda(\pi) \in \mathbb{N}$.

Note: if $\pi_1 \neq \pi_2$, then $p(\pi_1) \not\sim p(\pi_2)$.

Question. Can we drop the assumption that $\mathcal{O}$ is a PID (having a similar proof as above)? Can we replace $\mathcal{O}$ with (any) order $R \subseteq \mathcal{O}$?

3.1. Reducibility of polynomials

- Our goal

Problem. (classical) Let A be an integral domain and consider

$$A[X] = A[X_1, \ldots, X_n], \quad \text{ring of } A\text{-polynomials}$$

Question. When a particular $f \in A[X]$ cannot be written as $f = gh$ for some non-constant $g, h \in A[X]$?

Gauss: irreducibility of cyclotomic polynomials; Schönemann irreducibility criterion; Eisenstein criterion,...

Dumas: generalized E. criterion (via Newton polygons method)

Thm. (Eisenstein-Dumas criterion)
Let $f = c_n X^n + \cdots + c_1 X + c_0 \in \mathbb{Z}[X]$. *Suppose there is a prime* $p \in \mathbb{N}$ *such that:*

(1) $\mathrm{ord}_p(c_n) = 0$,

(2) $\gcd(n, \mathrm{ord}_p(c_0)) = 1$, *and*

(3) $(n-j)\,\mathrm{ord}_p(c_0) \leq n\,\mathrm{ord}_p(c_j)$ *for* $j = 1, \ldots, n-1$.

Then f *is irreducible over* $\mathbb{Q}$.

Remark. By the Gauss lemma, instead of $(\mathbb{Z}, \mathbb{Q})$ we can consider $(A, \mathcal{Q}(A))$ for A any UFD. ($\mathcal{Q}(A)$ is the field of quotients)

Goal. To generalize the above criterion for some non-UFD integral domains; e.g., orders R in number fields $\mathbb{K}$.

Example. Let $\mathbb{K} = \mathbb{Q}(\sqrt{10})$; here $\mathcal{O} = \mathbb{Z}[\sqrt{10}]$ is *not* a UFD. Suppose $f \in \mathbb{Z}[X]$ is of degree $n \leq 7$ and that for a rational prime $1 < p < 31$ the conditions (1)–(3) of the E-D criterion are fulfilled. Then f is irreducible over $\mathcal{O}$.

Remark. For our purpose we should have a good supply of prime elements in R!

- Dumas valution

$\Gamma = (\Gamma, +, \succeq)$, a totally ordered monoid with $\succeq$ monomial (i.e., for $a, b, c \in \Gamma$, $a \succeq b \;\Rightarrow\; a + c \succeq b + c$); e.g.

$$\Gamma = \mathbb{N}_0.$$

In the obvious way define totally ordered monoid extensions

$$\Gamma^{-\infty} = \Gamma \cup \{-\infty\} \quad \text{and} \quad \Gamma^{+\infty} = \Gamma \cup \{+\infty\}.$$

Def. Let R be an integral domain. A map

$$\omega : R \to \Gamma^{-\infty}$$

will be called a Γ-*Dumas valuation of the first kind* if for all $x, y \in R$ the following hold:

(D0) $\omega(x) \succeq 0_\Gamma$ if $x \neq 0$;

(D1) $\omega(xy) = \omega(x) + \omega(y)$;

(D2-1) $\omega(x) = -\infty$ if and only if $x = 0$;

(D3-1) $\omega(x + y) \preceq \max\{\omega(x), \omega(y)\}$, with equality if $\omega(x) \neq \omega(y)$.

A map

$$\omega : R \to \Gamma^{+\infty}$$

will be called a Γ-*Dumas valuation of the second kind* if for all $x, y \in R$ we have (D0), (D1) and also

(D2-2) $\omega(x) = +\infty$ if and only if $x = 0$;

(D3-2) $\omega(x + y) \succeq \min\{\omega(x), \omega(y)\}$, with equality if $\omega(x) \neq \omega(y)$.

!!! We say just *Dumas valuation* if $\Gamma = \mathbb{N}_0$.

Example. (1) A int. domain, $R = A[X] = A[X_1, \ldots, X_n]$. For any $\boldsymbol{\nu} = (\nu_1, \ldots, \nu_n) \in \mathbb{N}_0^n$ define the $\boldsymbol{\nu}$-*weight* of $I = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$ as

$$|I|_{\boldsymbol{\nu}} = \nu_1 i_1 + \cdots + \nu_n i_n \in \mathbb{N}_0.$$

For $n \geq 2$ and fixed $\boldsymbol{\nu} \in \mathbb{N}_0^n$ define the $\boldsymbol{\nu}$-*degree* of a nonzero polynomial $f = \sum_I a_I X^I \in A[X]$ as

$$\deg_{\boldsymbol{\nu}} f = \max\{|I|_{\boldsymbol{\nu}} \mid a_I \neq 0\}.$$

Claim 1. The map $\deg_\nu : R \to \mathbb{N}_0^{-\infty}$ is a Dumas valuation of the first kind.

(2) Let R be a Noetherian int. domain, or a UFD, and take a prime $p \in \operatorname{Pr} R$.

Claim 2. Define (standardly) a map $\operatorname{ord}_p : R \to \mathbb{N}_0^{+\infty}$, where we put $\operatorname{ord}_p(0) = +\infty$. Then ord_p is a Dumas valuation of the second kind.

Remark. For an int. domain A and $R = A[X]$ one can define the so-called *ν-codegree* map

$$\operatorname{codeg}_\nu : R \to \mathbb{N}_0^{+\infty}, \quad \operatorname{codeg}_\nu f = \min\{|I|_\nu \mid a_I \neq 0\}.$$

This is also a Dumas valuation of the second kind.

- Some results

Conjecture. *Let R be an int. domain, $n > 1$ and $\varphi_0, \varphi_1, \ldots, \varphi_n \in R$. Let ω be a Dumas valuation on R. Assume:*

(A) $\omega(\varphi_n) = 0$, $\omega(\varphi_0) \in \mathbb{N}$ *and* $\gcd(n, \omega(\varphi_0)) = 1$.

Also assume one of the following two possibilities:

(B1) ω *is of the first kind and we have the inequalities*

$$n\omega(\varphi_j) \leq (n-j)\omega(\varphi_0) \quad \text{for } j = 1, \ldots, n-1;$$

or

(B2) ω *is of the second kind and we have the inequalities*

$$n\omega(\varphi_j) \geq (n-j)\omega(\varphi_0) \quad \text{for } j = 1, \ldots, n-1.$$

Then $f = \varphi_n X^n + \cdots + \varphi_1 X + \varphi_0$ is irreducible in $R[X]$.

Main thm. *For ω of any kind and $n \leq 7$ the Conjecture is true.*

Now, which integral domains R to consider (when classical E-D criterion cannot help)?

Consider: $\mathbb{K}$ a number field, $\mathcal{O} = \mathcal{O}_{\mathbb{K}}$ and

$$R = \text{an order in } \mathbb{K} \text{ s.t. } R \text{ is not a UFD}$$

(i.e., $R \neq \mathcal{O}$ or $R = \mathcal{O}$ when $h_{\mathbb{K}} > 1$).

Thm. *Let R be an order in a number field $\mathbb{K}$. Suppose $f = c_n X^n + \cdots + c_1 X + c_0 \in R[X]$, polynomial in one variable, of degree $n \leq 7$. Suppose there is $p \in \operatorname{Pr} R$ s.t.:*

(1) $\operatorname{ord}_p(c_n) = 0$,

(2) $\gcd(n, \operatorname{ord}_p(c_0)) = 1$, *and*

(3) $(n-j)\operatorname{ord}_p(c_0) \leq n \operatorname{ord}_p(c_j)$ *for* $j = 1, \ldots, n-1$.

Then f is irreducible over R.

Cor. *Suppose the setting of the last Theorem. Suppose $p \in \mathbb{N}$ is a prime number which is inert in $\mathbb{K}$ and it satisfies the conditions (1)–(3). Then f is irreducible over $\mathcal{O}$.*

(!!! Remember Example with $\mathbb{K} = \mathbb{Q}(\sqrt{10})$.)

Remark. By considering Dumas valuations of both the first and second kind on $R = A[X_1, \ldots, X_n]$ one can get some results about irreducibility of polynomials over R in $n \geq 2$ variables. (Here A is an integral domain.)

3.2. On "generalized modular groups" and Frattini subgroups

- Preliminaries

G any group, $\quad \operatorname{Max} G =$ the set of all maximal subgroups

$\Phi(G) = \bigcap_{\operatorname{Max} G} M$, $\quad$ *Frattini subgp* $\quad (\Phi(G) = G$ if $\operatorname{Max} G = \emptyset)$.

Goal. To understand $\operatorname{Max} G$ and $\Phi(G)$ for particular G's.

Our setting. $\mathbb{K}$ a number field, $\mathcal{O} = \mathcal{O}_{\mathbb{K}}$. Define

$$G^{(n)} = \mathrm{SL}_n(\mathcal{O}),$$

the n-th *generalized modular group* attached to $\mathbb{K}$.

Notation. R int. domain

$\mathrm{e}_{ij} =$ standard matrix with 1 on place (i,j) and 0 elsewhere

$E_{ij}(x) = I_n + x\mathrm{e}_{ij} \in \operatorname{Mat}_n(R)$, $\quad$ elementary matrices

$\mathcal{E}_n(R) =$ the subgroup of $\mathrm{SL}_n(R)$ generated by all elementaries.

- Case $n = 2$ $\qquad G_R = \mathrm{SL}_2(R)$

Def. For any $N \in R^\times \setminus R^*$ define a *Hecke congruence group of level* N by

$$\Gamma_0^R(N) = \left\{ A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G_R \mid c \equiv 0 \pmod{N} \right\}.$$

Write $\Gamma_0(N)$ when $R = \mathcal{O}$.

The claim (i) of the following prop. generalizes the fact that

$$\mathrm{SL}_2(\mathbb{Z}) = \langle S, T \rangle, \quad \text{where } S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T = E_{12}(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Prop.

(i) *Suppose R is a Euclidean domain with $\lambda : R^\times \to \mathbb{N}_0$. Then $\mathcal{E}_2(R) = G_R$.*

(ii) *Suppose R is a Euclidean domain or $R = \mathcal{O}$ s.t. it is a PID and $\mathcal{O}^*$ is infinite. Then for every $p \in \mathrm{Pr}\, R$ the Hecke group $\Gamma_0^R(p) \in \mathrm{Max}\, G_R$.*

Sketch of the proof.

(i) Assume we have $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_R \setminus \mathcal{E}_2(R)$. Then necessarily $c \neq 0$. We can choose A s.t. $\lambda(c)$ is minimal possible. Then we get a contradiction...

(ii) We have $\mathcal{E}_2(R) = G_R$ (Vaserstein's theorem; a stronger result by Morgan, Rapinchuk and Sury)
Assume there is a subgroup $\Gamma_0^R(p) \subset H \leq G_R$. Let $B = \begin{pmatrix} \alpha & \beta \\ w & \gamma \end{pmatrix} \in H \setminus \Gamma_0^R(p)$ be arbitrarily chosen.

1. Case $w \in R^*$. Now we easily get that $S \in H$ and then $H = G_R$.

2. Case $w \notin R^*$. We show that $(w) + (\gamma p) = R$. Thus $sw + tp\gamma = 1$ for some $s, t \in R$. Then for $M = \begin{pmatrix} s & -\gamma \\ tp & w \end{pmatrix} \in \Gamma_0^R(p)$ we have $BM = \begin{pmatrix} * & * \\ 1 & * \end{pmatrix} \in H \setminus \Gamma_0^R(p)$. So we are again in Case 1.

Now we are ready for the following.

Thm. 4. *Suppose R is an integral domain from any of the following two classes of rings:*

(I) *R is a Euclidean domain having infinitely many non-associated prime elements; or*

(II) *R is the ring of integers $\mathcal{O}$ of some number field such that it is a PID and the group of invertibles $\mathcal{O}^*$ is infinite.*

Then the Frattini subgroup $\Phi(G_R)$ is contained in the center $\mathcal{Z}(G_R) = \{\pm I\}$.

Sketch of the proof.

For any $p \in \operatorname{Pr} R$ we know that $\Gamma_0^R(p) \in \operatorname{Max} G_R$. Also the "transposed groups" $(\Gamma_0^R)^-(p) \in \operatorname{Max} G_R$. Take any $T \in \Phi(G_R)$. As $\widehat{\operatorname{Pr}} R$ is infinite (Thm. 2) we obtain that $T = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$, for some $t \in R^*$. By a little work: $T \in \{\pm I\}$.

———————————–

Remark. (1) The only number fields having class number 1 that are not covered by our theorem are the imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ for $d \in \{19, 43, 67, 163\}$. (This does not mean that for these fields our theorem does not hold!)
(2) Recall that $\mathbb{F}[X]$ is Euclidean for $\mathbb{F}$ a field. Also every discrete valuation ring is Euclidean. Assuming the extended Riemann hypothesis, if for a number field $\mathbb{K}$ the corresponding $\mathcal{O}$ is a PID having $\mathcal{O}^*$ infinite, then $\mathcal{O}$ is Euclidean.

- Case $n = 3$ $\qquad G_R = \mathrm{SL}_3(R)$

Def. For any $N \in R^\times \setminus R^*$ define

$$\Gamma^R_{[1,2]}(N) = \{(a_{ij}) \in G_R \mid a_{21} = a_{31} \equiv 0 \pmod{N}\},$$
$$\Gamma^R_{[2,1]}(N) = \{(a_{ij}) \in G_R \mid a_{31} = a_{32} \equiv 0 \pmod{N}\},$$

and also $\Gamma^R_0(N) = \Gamma^R_{[1,2]}(N) \cap \Gamma^R_{[2,1]}(N)$.

Lemma. *These are subgroups of G_R.*

Remark. For any $n \geq 2$, $N \in R^\times \setminus R^*$ and a k-tuple $\nu = [n_1, \ldots, n_k]$ of positive integers n_i satisfying $n_1 + \cdots + n_k = n$ we can define certain congruence subgroups $\Gamma^R_\nu(N)$, of level N and type ν...

Prop.

(i) *Suppose R is a Euclidean domain with $\lambda : R^\times \to \mathbb{N}_0$. Then $\mathcal{E}_3(R) = G_R$.*

(ii) *Suppose R is a Euclidean domain or $R = \mathcal{O}$ s.t. it is a PID. Then for every $p \in \Pr R$ the congruence subgroups $\Gamma^R_{[1,2]}(p)$ and $\Gamma^R_{[2,1]}(p)$ are maximal subgroups of G_R.*

Comments on the proof.

(i) This time our proof is considerably more involved than for $n = 2$.

(ii) For the case $R = \mathcal{O}$ we use a result due to Bass, Milnor and Serre who proved that $\mathcal{E}_n(\mathcal{O}) = G_{\mathcal{O}}^{(n)}$ for $n \geq 3$. Then we prove in a non-trivial way that (ii) holds.

———————-

We conclude with the following analogue of Thm. 4.

Thm. 5. *Suppose R is an integral domain from any of the following two classes of rings:*

(I) *R is a Euclidean domain having infinitely many non-associated prime elements; or*

(II) *R is the ring of integers $\mathcal{O}$ of some number field such that it is a PID.*

Then the Frattini subgroup $\Phi(G_R)$ is contained in the center $\mathcal{Z}(G_R) = \boldsymbol{\mu}_3(R)I$.

In particular if R equals the ring of integers $\mathcal{O}$ of a number field $\mathbb{K}$ which is a subfield of $\mathbb{R}$, or more generally $\mathbb{K} \subseteq \mathbb{C}$ is such that $-1/2 + i\sqrt{3}/2 \notin \mathcal{O}$, then $\Phi(G_{\mathcal{O}}) = \{I\}$.

Some references

1. H. Abels and G. A. Noskov, *The Frattini subgroup of a Lie group and the topological rank of a Lie group*, J. Algebra 640 (2024), 326–367.
2. H. Bass, J. Milnor and J.-P. Serre, *Solution of the congruence subgroup problem for* SL_n $(n \geq 3)$ *and* Sp_{2n} $(n \geq 2)$, Inst. Hautes Études Sci. Publ. Math. 33 (1967), 59–137.
3. A. V. Morgan, A. S. Rapinchuk and B. Sury, *Bounded generation of* SL_2 *over rings of S-integers with infinitely many units*, Algebra and Number Theory 12 (2018), 1949–1974.
4. B. Š., *On prime elements in commutative domains*, Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. 28(558) (2024), 223–243.
5. B. Š., *A generalization of Eisenstein-Dumas criterion*, preprint.
6. B. Š., *On maximal subgroups, generalized modular groups and Frattini subgroups*, preprint.

Thank you!

(for your patience)