1. Classical modular group, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $ad-bc=1$ a,b,c,d integers (rational), generated by $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, acts on upper complex halfplane.

Hilbert modular group: Totally real number field K of degree n, elements: $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $\alpha\delta - \beta\gamma = 1$ $\alpha, \beta, \gamma, \delta$ integers in K. Parabolic subgroup Γ_∞ elements $\begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}$, ω integers in K, acts on product of n upper complex halfplanes.

2. Hecke 1935 asked when does $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -\frac{1}{c} \\ c & 0 \end{pmatrix}$ generate a discrete group? He showed this was the case if either $c = 2\cos\frac{\pi}{q}$, q integer ≥ 3, or $c \geq 2$.

More generally we may ask: <u>When does $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ generate a discrete group?</u>

Or for general n: Given a lattice of translations in euclidean n-space, with elements ω (consisting each of n components $\omega^{(i)}$) are generated by n linearly independent elements $\xi_1, \dots, \xi_n$ (so that the matrix $(\xi_j^{(i)})$ is non-singular). By Γ_∞ we will now denote the group with elements $\begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}$, generated by $\begin{pmatrix} 1 & \xi_j \\ 0 & 1 \end{pmatrix}$ for $j = 1, \dots, n$. Put $\mathfrak{L} = (\xi_j^{(i)})$

We assume further that the projection of this lattice on any of the subspaces arising by omitting some of the n components is not discrete, (or what is the same: no $\omega^{(i)} = 0$ unless $\omega = 0$, that is: all components vanish if one does). We may now ask: if we adjoin an element $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ (to be understood as a set of n components $\begin{pmatrix} \alpha^{(i)}, & \beta^{(i)} \\ \gamma^{(i)}, & \delta^{(i)} \end{pmatrix}$ with $\alpha\delta - \beta\gamma = 1$, we do not assume the numbers to lie in any algebraic field here, just that they are real numbers) to the group with elements $\begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}$ when is the resulting group discrete?

Notations: $N(\alpha) = \prod_{i=1}^{n} |\alpha^{(i)}|$;

$D = \| \xi_j^{(i)} \| = \|\Omega\|$.

Minkowski: For $t_i > 0$ and $\prod_{i=1}^{n} t_i \geq D$ $\exists\ \omega \neq 0$ with $|\omega^{(i)}| \leq t_i$

Can first show that either all $\gamma^{(i)} = 0$, or all $\gamma^{(i)} \neq 0$.

First case is fairly trivial to handle, so we shall consider second case, all $\gamma^{(i)} \neq 0$

We can then write

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = S^{\frac{\alpha}{\gamma}} T_\gamma S^{\frac{\delta}{\gamma}},$$

where $S^{\frac{\alpha}{\gamma}} = \begin{pmatrix} 1 & \frac{\alpha}{\gamma} \\ 0 & 1 \end{pmatrix}$, $T_\gamma = \begin{pmatrix} 0 & -\frac{1}{\gamma} \\ \gamma & 0 \end{pmatrix}$.

Considering strings of elements

$$S^{\omega_0} M S^{\omega_1} M^{-1} S^{\omega_2} M \cdots S^{\omega_k} M^{(-1)^k} S^{\omega_{k+1}}$$

we see that it equals

$$\pm S^{\frac{\alpha}{\gamma}} \left(S^{\omega_0} T_\gamma S^{\omega_1} T_\gamma \cdots S^{\omega_k} T_\gamma S^{\omega_{k+1}} \right) S^{-\frac{\delta}{\gamma}},$$

From which we can conclude: <u>We can only get a discrete group by adjoining M if we also get a discrete group by adjoining T_γ.</u>

Writing

$$M_k = T_\gamma S^{\omega_1} T_\gamma \cdots S^{\omega_{k-1}} T_\gamma = \begin{pmatrix} \alpha_k & \beta_k \\ \gamma_k & \delta_k \end{pmatrix}$$

we have recursion formulas

$\alpha_{k+1} = \gamma \omega_k \alpha_k - \alpha_{k-1}$; $\gamma_{k+1} = \gamma \omega_k \gamma_k - \gamma_{k-1}$,

$\alpha_0 = 1$, $\alpha_1 = 0$, $\gamma_0 = 0$, $\gamma_1 = \gamma$.

$\gamma_2 = \omega_1 \gamma^2$, $\gamma_3 = \omega_1 \omega_2 \gamma^3 - \gamma$, $\gamma_4 = \omega_1 \omega_2 \omega_3 \gamma^4 - (\omega_1 + \omega_3)\gamma^2$; $\alpha_2 = -1$, $\alpha_3 = -\gamma \omega_2$,

$\alpha_4 = -\omega_2 \omega_3 \gamma^2 + 1$.

For all $\omega \neq 0$, we have $N(\omega\gamma) \geq 1$.

In particular $N(\gamma) \geq \frac{1}{D}$.

We shall first investigate structure of lattice ω, using the principle that in any compact region there can only be finitely many different elements of a discrete group.

We construct pairs ω_1, ω_2 so that $|\omega_1^{(i)} \omega_2^{(i)}| \leq D^{\frac{2}{n}}$ and such that for $1 \leq i < j \leq n$ we have

$|\omega_1^{(i)}| \leq T D^{\frac{1}{n}}$, $|\omega_1^{(j)}| \leq \frac{1}{T} D^{\frac{1}{n}}$;

$|\omega_1^{(n)}| \leq D^{\frac{1}{n}}$ for $n \neq i$ or j, for ω_2 we reverse the (two first) inequalities.

Looking at M_3 with $\gamma_3 = \omega_1 \omega_2 \gamma^3 - \gamma$ we see as $T \to \infty$ this remains bounded (and also bounded away from 0 since $N(\gamma_3) \geq \frac{1}{D}$). Now there $\exists\, \omega, \omega'$ such that $S^{\omega} M_3 S^{\omega'} = \begin{pmatrix} 1+O(|\gamma_3|) & O(1+|\gamma_3|) \\ \gamma_3 & 1+O(|\gamma_3|) \end{pmatrix}$ which then lies in a compact region of γ_3 does. Thus as $T \to \infty$, we must get the same element $S^{\omega} M_3 S^{\omega'}$ infinitely often.

Thus we get relations of the form ω_1, ω_2
$\omega_1 \omega_2 - \omega_1' \omega_2' = 0$, where say ω_1, ω_2 correspond to a T which we make very large, while $\omega_1' \omega_2'$ correspond to a T' kept fixed. This gives a relation of the form

$$\sum_{1 \le k,\ell \le n} c^{(i,j)}_{k,\ell} \xi_k \xi_\ell = 0$$

with integral coefficients $c^{(i,j)}_{k,\ell}$
As T is made large we can find asymptotic expressions for the $c^{(i,j)}_{k,\ell}$ and deduce that the $\frac{n(n-1)}{2}$ relations we get for $1 \le i < j \le n$ are linearly independent so we can solve with respect to $\xi_k \xi_\ell$ with $1 \le k \le \ell \le n-1$, and get

$$\xi_k \xi_\ell = \sum_{r=1}^{n} d_r^{k,\ell} \xi_r \xi_n$$

with rational coefficients $d_r^{k,\ell}$. Writing $\xi_k = \xi_k \xi_n$ (so $\xi_n = 1$), we get

$$\xi_k \xi_\ell = \sum_{r=1}^{n} d_r^{k,\ell} \xi_r$$

From this we easily see that each $\frac{\omega}{\omega_n}$ satisfies a polynomial equation of degree n at most

Since any power can be expressed as

$$\frac{\omega^m}{\xi_n^m} = \sum_{r=1}^{n} e_{r,m}^{\omega}\, \xi_r$$

with rational coefficients e, and the $(n+1)$ expressions for $0 \le m \le n$ can not be linearly independent. We also see that taking (as we can) an ω such that $\frac{\omega}{\xi_n}$ generates the field containing all the ξ_r, $\frac{\omega}{\xi_n}$ then must satisfy an equation of degree exactly n. Thus there exists a totally real field K of degree n such that the ratios of any two ω's lie in this field and the components $\left(\frac{\omega_1}{\omega_2}\right)^{(i)}$ are simply the various conjugates.

It is easily seen that this means that we by a suitable group conjugacy with a suitable $\begin{pmatrix} \rho & 0 \\ 0 & \frac{1}{\rho} \end{pmatrix}$ can bring our lattice on such a form that all ω lie in K and that it contains all integers in K.

We next wish to show that $\chi\omega$ is an algebraic integer and $(\chi\omega)^2$ is in the field K.

We assume that we have (by a conjugacy) brought our lattice to the form that it contains all integers in K. We wish first to show that γ^2 lies in K. We again look at the elements of form

$$M_3 = T_\gamma S^{\omega_1} T_\gamma S^{\omega_2} T_\gamma$$

we have seen that we could choose ω_1, ~~and~~, ω_2 and ω_1', ω_2' such that they have the same product $\omega_1\omega_2 = \omega_1'\omega_2'$ and so the same $\gamma_3 = \omega_1\omega_2\gamma^3 - \gamma$ as we let our T in the construction $\to \infty$, we see that we must have identities

$$M_3 = S^{\omega_0} M_3' S^{\omega_3}$$

so

$$\alpha_3 = \alpha_3' + \omega_0\gamma_3$$

inserting the values of α_3, α_3' and γ_3 we get

$$-\gamma\omega_2 = -\gamma\omega_2' + \omega_0\omega_1\omega_2\gamma^3 - \gamma\omega_0$$

or

$$\gamma^2 = \frac{\omega_0 + \omega_2' - \omega_2}{\omega_0\omega_1\omega_2}$$

thus γ^2 is in K.

We now assume γ^2 is not an integer in the field K and wish

to get a contradiction. If our γ^2 is not of the form $\frac{\rho}{\varkappa}$ where ρ and $\varkappa$ are in K and $(\rho, \varkappa) = 1$, we can pass to a new γ' of the form

$$\gamma' = \omega \gamma^{2^k}$$

where 2^k is larger than the class number of K, and choose the integer ω so that γ' can be written as $\frac{\rho}{\varkappa}$ with $(\rho, \varkappa) = 1$, and $\varkappa$ is not a unit. We now write γ instead of γ'. Forming again elements M_4 we have

$$\gamma_4 = \omega_1 \omega_2 \omega_3 \gamma^4 - (\omega_1 + \omega_3)\gamma^2$$

and $$\alpha_4 = -\omega_2 \omega_3 \gamma^2 + 1 .$$

If the ω's can be chosen so that

(*) $$\omega_1 \omega_2 \omega_3 \gamma^2 = \omega_1 + \omega_3$$

we see that

α_4 becomes $-\frac{\omega_3}{\omega_1}$, $\gamma_4 = 0$.

This would give a contradiction if $\frac{\omega_3}{\omega_1}$ is <u>not</u> a unit, since in upper triangular elements the diagonal elements must be units, since conjugation with such an element must preserve the lattice.

(*) can be rewritten

$$\omega_1 \omega_2 \omega_3 \rho^2 = (\omega_1 + \omega_3) x^2,$$

we may choose ω_1 as a unit η, and ω_3 as divisor δ of x^2 and not a unit. We see that if

$$\eta + \delta \equiv 0 \pmod{\rho^2}$$

ω_2 can also be chosen as an integer in K_n and we would get an contradiction.

Obviously it would help if x^2 has many divisors. So we try to pass from over $\gamma = \frac{\rho}{x}$ to a γ_k for which a solution of the congruence can be assured; we write

$$\gamma_k = \frac{\rho_k}{x^k} \text{ and find}$$

$$\rho_{k+1} = \rho \omega_k \rho_k - x^2 \rho_{k-1},$$

$\rho_1 = \rho$, $\rho_2 = \rho^2 \omega_1$, $\rho_3 = \rho^3 \omega_1 \omega_2 - x^2 \rho$, ..

In general we write

$$\rho_{2k} = \rho^2 \Delta_{2k}, \quad \rho_{2k+1} = \rho \Delta_{2k+1}$$

and get:

$$\Delta_{2k+1} = \omega_{2k} \rho^2 \Delta_{2k} - x^2 \Delta_{2k-1}$$

$$\Delta_{2k+2} = \omega_{2k+1} \Delta_{2k+1} - x^2 \Delta_{2k}$$

or $\Delta_{2k+1} \equiv -\alpha^2 \Delta_{2k-1} \pmod{\rho^2 \Delta_{2k}}$,

$\Delta_{2k+2} \equiv -\alpha^2 \Delta_{2k} \pmod{\Delta_{2k+1}}$.

We try to select a sequence of Δ's satisfying these congruences, such that $\Delta_k = \eta_k \pi_k^{m_k}$, where η_k is a unit, π_k a representative of a principal primeideal of degree one (with norm p_k), such that π_{2k+2} is always a primitive root mod π_{2k+1}^2,

$\pi_{2k+1}^{p_{2k}-1} \not\equiv 1 \pmod{\pi_{2k}^2}$, $p_{2k+1} > N(\rho^2)$,

and

$\eta_{2k+1} \pi_{2k+1} \equiv -\alpha^2 \eta_{2k-1} \pi_{2k-1}^{m_{2k-1}} \pmod{\rho^2 \pi_{2k}^2}$.

This can always be done, but we can also always select our π_k such that any L-function with a character mod π_k^2 or $\rho^2 \pi_k^2$ which is not the restriction of a character mod ρ^2 has no zero in the region $|t| < p_k^{10}$, $\sigma > 1 - \delta$ where δ is a small positive constant dependent on K, since a density result shows that the π for which this does not hold form a very thin set.

We can then show that we can select our π_k such that

$$p_{2k+1} \leq \max\left(p_{2k}^{A}, C(\rho,\delta)\right)$$

where A is constant depending on K, while

$$p_{2k+2} \leq \max\left(p_{2k+1}^{\varepsilon}, C(\rho,\delta,\varepsilon)\right)$$

where ε is an arbitrary chosen positive number.

This gives

$$p_{k+2} \leq \max\left(p_k^{A\varepsilon}, C'(\rho,\delta,\varepsilon)\right),$$

so by choosing $\varepsilon \leq \frac{1}{A}$ we see that the p_k do not grow over all bounds, but stay bounded.

We now look at

$$\gamma_{2k+1} = \rho^{m_{2k+1}} \frac{\pi_{2k+1}}{\eta^{2k+1}} \eta_{2k+1}.$$

Taking an arbitrary unit of infinite order η, we see that η^{s} represents at least $p_{2k+1}^{2m_{2k+1}-n}$ different residue-

classes mod $(\rho^2 \pi_{2k+1}^{2m_{2k+1}})$ where r is the (highest) power of π_{2k+1} that divides $\eta^{p_{2k+1}-1} - 1$; this r is bounded since p_{2k+1} is. Now consider the sets $\eta^s x^t$ with $0 \le t \le 4k+2$, they represent at least $(4k+2) p_{2k+1}^{2m_{2k+1} - r}$ residue classes. For $4k+2 > p_{2k+1}^{r} N(\rho^2)$ this is larger than the total number of residues $(\mathrm{mod}\ \rho^2 \pi_{2k+1}^{2m_{2k+1}})$, thus there is duplication and since two with the same t are not congruent we get

$$\eta^s x^t \equiv \eta^{s'} x^{t'} \left(\mathrm{mod}\ \rho^2 \pi_{2k+1}^{2m_{2k+1}}\right)$$

and so

$$x^{|t-t'|} \equiv \eta^{s''} \left(\mathrm{mod}\ \rho^2 \pi_{2k+1}^{2m_{2k+1}}\right)$$

here $1 \le |t-t'| < 4k+2$

so we have our contradiction.

Thus our original γ must be an integer such that γ^2 is in K.

Going back to the original $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, and forming higher powers M^k, we easily see that the eigenvalues of M must be algebraic integers (units but not in K in general), and the trace of M, $\alpha+\delta$ must be an integer whose square is in K.

Since the trace of $S^\omega M$ must also be integral we get that $\gamma\omega$ is an algebraic integer whose square is in K, and that $(\alpha+\delta)\gamma\omega$ also is an integer in K. These statements are in a form that is invariant under the conjugacies by upper triangular elements.

It is not hard to show that they are also sufficient to ensure that the adjunction of M to the parabolic group produces a discrete group.

The solution for $n=1$, is much simpler, and rather different. Finally, if we replace some or all copies of $SL(2,R)$ with $SL(2,C)$, things are very similar as long as $n \geq 2$. The case $n=1$ however, seems rather intractable in general