Геометрия, арифметика и динамика дискретных групп.

Богачев Николай Владимирович
(Сколтех & МФТИ)

Лекция 11

I Введение (было)

II Топология (была)

III Риманова геометрия (была)

IV Действия групп, геометрическая теория групп, дискретные подгруппы групп Ли. (было)

V Гиперболические поверхности, многообразия, орбифолды. Группы отражений. Решетки в $\mathrm{Isom}(E^n)$, $\mathrm{Aff}(\mathbb{R}^n)$ (было)

VI Основные концепции геометрической теории групп: QI = квазиизометрии; граф Кэли; лемма Шварца–Милнора; δ-гиперболичность; группы, гиперболические по Громову.

VII Деформации (H^2) и жесткость ($H^{\geq 3}$): штаны pants decomposition; mapping class groups; пр-ва модулей; пр-во Тайхмюллера; группа Торелли I_g и ядро Джонсона K_g; твисты Дэна Dehn twists; curve graph и гиперб-по Громову; формулировки теорем жесткости (Мостов, Прасад, Маргулис)

Комментарии к пред. лекциям:

- $\Gamma < G$ — реш. гр. Ли. Если G некомпактна, то $\Gamma \supset F_n$, $n \geq 2$, и, след., не разр.
- $M = H^n/\Gamma$ с каспом. Сечения каспа = $(n-1)$-мерный тор T^{n-1}. Таким обр., $\Gamma > \mathbb{Z}^{n-1} \Rightarrow$ НЕ гипрб. по Громову при $n \geq 3$.

VIII Теоремы жесткости Мостова, Прасада и Маргулиса. Доказательство теоремы жесткости Мостова для компактных гиперболических мног-ий.

IX Арифметические группы: общая теория

⓪ Неформальное введение

Арифметические группы — это, грубо говоря, группы целых точек.
Например, модулярная группа $PSL_2(\mathbb{Z})$; группа $SL_n(\mathbb{Z})$; или группа целочисленных автоморфизмов (группа единиц) квадр. форм: пусть $q(x) = \sum_{i,j \le n} q_{ij} \cdot x_i \cdot x_j$, где $q_{ij} = q_{ji} \in \mathbb{Z}$.
Тогда можно рассм. $\Gamma = O_q(\mathbb{Z}) = \{A \in GL_n(\mathbb{Z}) \mid A^T Q A = Q = (q_{ij})\}$.
(Если $q \sim_{\mathbb{R}} (m,1)$, то $O'_q(\mathbb{Z}) < PO_{m,1}(\mathbb{R}) \cong \mathrm{Isom}(\mathbb{H}^m)$)

① Поля алгебр. чисел

Основные поля: $k = \mathbb{Q}(\{t_j \in \mathbb{C} \mid j \in \Omega,\ \mathrm{card}(\Omega) < +\infty\})$.
Здесь $k = \min\{k' \mid k' \ni t_1, \dots, t_N\}$. Обычно, t_j — корни $p_j(t)$ с коэфф. из $\mathbb{Q}$. Тогда $k = \mathbb{Q}(\alpha)$, где $f(\alpha) = 0$ для
(polynomials) $f \in \mathbb{Q}[t]$ — неприв. многочлен со ст. коэфф. 1.
В этом случае степень поля есть $\deg(k) := [k:\mathbb{Q}] = \deg(f)$.
Помимо α миним. многочлен f имеет и другие корни. Всего имеем r_1 вещ. и $2r_2$ комплексных корней (компл. входят
real places / complex places
парами β и $\bar{\beta}$). Эти корни считаем сопряж. друг другу:
поля $\mathbb{Q}(\alpha_1)$ и $\mathbb{Q}(\alpha_2)$ изоморфны, и при всех вложениях $\sigma: k \longrightarrow \mathbb{C}$ число $\sigma(\alpha)$ тоже есть корень $f(t)$.
Все эти вложения образуют конечную группу Галуа $\mathrm{Gal}(k/\mathbb{Q})$.
Для всякого $\beta \in k$ можно определить норму и след:

$$N_{k/\mathbb{Q}}(\beta) = \prod_{j=1}^{d} \sigma_j(\beta) \quad \text{и} \quad Tr_{k/\mathbb{Q}}(\beta) = \sum_{j=1}^{d} \sigma_j(\beta).$$

В нашем $(k=\mathbb{Q}(\alpha))$ случае $f(\alpha)=0$, где $f(t)=t^d+\underbrace{f_{d-1}}t^{d-1}+\ldots+f_1t+f_0$.

Тогда $N(\alpha)=\pm f_0$ и $Tr(\alpha)=\pm f_{d-1}$.

Набор $\{\beta_1,\ldots,\beta_d\}$ явл. базисом поля k над $\mathbb{Q}$, если числа β_j лин. нез. над $\mathbb{Q}$, что равносильно тому, что $\det[\sigma_i(\beta_j)]\neq 0$.

Для $k=\mathbb{Q}(\alpha)$ базисом является $\{1,\alpha,\alpha^2,\ldots,\alpha^{d-1}\}$.

Дискриминант $\{\beta_1,\ldots,\beta_d\}$ есть $\operatorname{disc}\{\beta_1,\ldots,\beta_d\}=\det[\sigma_i(\beta_j)]^2=\det(Tr(\beta_i\beta_j))$

Заметим, что $\operatorname{disc}\{1,\alpha,\ldots,\alpha^{d-1}\}=\det(\alpha_i^j)^2=\prod\limits_{1\le i<j\le d}(\alpha_i-\alpha_j)^2$.

Опр. $k\subset\mathbb{R}$ - вп. вещ., если $r_2=0$ ($\Leftrightarrow \sigma(k)\subset\mathbb{R}$ $\forall\sigma: k\hookrightarrow\mathbb{C}$).

Лемма $\operatorname{disc}\{\alpha_1,\ldots,\alpha_d\}$, $N_{k/\mathbb{Q}}(\alpha)$ и $Tr_{k/\mathbb{Q}}(\alpha)$ - инварианты группы Галуа $Gal(k/\mathbb{Q})$, т.е. лежат в $\mathbb{Q}$, причем $N(\alpha\cdot\beta)=N(\alpha)\cdot N(\beta)$.

Опр. Число $\alpha\in k$ - алгебр. целое над $\mathbb{Z}$, если $\exists g\in\mathbb{Z}[t]: g(\alpha)=0$ и $g(t)=t^m+a_{m-1}t^{m-1}+\ldots+a_0$ (т.е. $a_j\in\mathbb{Z}$). Кольцо целых поля k обозн. через $\mathcal{O}_k=\{\alpha\in k\mid \alpha$ цел над $\mathbb{Z}\}$. Это замыкание $\mathbb{Z}$. Аналогично определяется замыкание подкольца R_1 в комм. кольце R_2.

Всякое поле k есть поле частных своего кольца $\mathcal{O}_k$, след., сущест. $\alpha\in\mathcal{O}_k$, т.что $k=\mathbb{Q}(\alpha)$. Если $k=\mathbb{Q}(\alpha)$, где $\alpha\in\mathcal{O}_k$, то $\mathbb{Z}[\alpha]\subset\mathcal{O}_k$, т.е. $\operatorname{rank}(\mathcal{O}_k)\geq d$. Пусть $\delta=\operatorname{disc}\{1,\alpha,\ldots,\alpha^{d-1}\}$ в этом случае, тогда $\mathcal{O}_k\subset\frac{1}{\delta}\mathbb{Z}[\alpha]$, т.е $\operatorname{rank}(\mathcal{O}_k)=d$. Заметим, что все целые базисы имеют равные дискр. (матрицы перехода рац. и имеют $\det=\pm1$).

Опр. $\delta_k=\operatorname{disc}\{$целый базис$\}$ — дискр. поля k.

Примеры 1) $k=\mathbb{Q}(\sqrt{2})=\mathbb{Q}[t]/(t^2-2)$. Здесь базис $\{1,\sqrt{2}\}$ (корни $\beta_{1,2}=\pm\sqrt{2}$)

$[k:\mathbb{Q}]=2$; $Gal(k/\mathbb{Q})\cong\mathbb{Z}_2=\mathbb{Z}/2\mathbb{Z}$, т.е. $\sigma_1(a+b\sqrt{2})=a+b\sqrt{2}$, $\sigma_2(a+b\sqrt{2})=a-b\sqrt{2}$.

Ясно, что $\mathbb{Q}(\sqrt{2})$ - вп. вещ. Найдем все инварианты.

$N(a+b\sqrt{2})=(a+b\sqrt{2})(a-b\sqrt{2})=a^2-2b^2$. Напр., $N(\sqrt{2})=-2$; $N(1+\sqrt{2})=-1$.

$Tr(a+b\sqrt{2})=2a$; $Tr(\sqrt{2})=0$.

$$\delta_k=\operatorname{disc}\{1,\sqrt{2}\}=\det{}^2\begin{pmatrix}1&\sqrt{2}\\1&-\sqrt{2}\end{pmatrix}=(-2\sqrt{2})^2=4\cdot 8=8=\det\begin{pmatrix}Tr(1)&Tr(\sqrt{2})\\Tr(\sqrt{2})&Tr(2)\end{pmatrix}\overset{\det(\operatorname{diag}(2,4))}{=}$$

Наконец, поскольку $\{1, \sqrt{2}\}$ – целый базис, то можно показать, что $\mathcal{O}_k = \mathbb{Z}[\sqrt{2}]$. Убедитесь, что $\forall x \in k \ \exists a, b \in \mathcal{O}_k : x = \frac{a}{b} = \frac{a_1 + a_2\sqrt{2}}{b_1 + b_2\sqrt{2}}$.

2) $k = \mathbb{Q}(\sqrt{5})$. Заметим, что "золотое сечение" $\varphi = \frac{1+\sqrt{5}}{2} \in \mathcal{O}_k$, но при этом $\varphi \notin \mathbb{Z}[\sqrt{5}]$. Т.е. $\mathbb{Z}[\sqrt{5}]$ не явл. алгебр.-замкнутым в k.
(Действит., $(2\varphi-1)^2 = 5$, т.е. $4\varphi^2 - 4\varphi + 1 = 5 \Leftrightarrow \varphi^2 - \varphi - 1 = 0$.)
На самом деле, $\{1, \varphi\}$ – $\mathbb{Z}$-базис для k и $\mathcal{O}_k = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] = \mathbb{Z}[\varphi]$.

3) $k = \mathbb{Q}(\sqrt{m})$, где $m \in \mathbb{Z}$ – свободно от квадратов. Для таких квадратичных полей имеем $\mathbb{Z}$-базис: $\{1, \alpha\}$, где $\alpha = \begin{cases} \sqrt{m}, & m \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{m}}{2}, & m \equiv 1 \pmod 4 \end{cases}$
В первом случае $\delta_k = 4m$, во втором $\delta_k = m$.

4). Заметим, что число $\cos\left(\frac{2\pi}{m}\right)$ (и $2\cos\frac{\pi}{m}$) явл. алгебр. целым (многочлены Чебышёва).
Рассм. $k = \mathbb{Q}(\cos\frac{\pi}{7})$ – поле степени 3. Его кольцо целых $\mathcal{O}_k = \mathbb{Z}\left[\cos\frac{2\pi}{7}\right]$.

5) Можно рассматривать также не вн. вещ. поля, напр. мнимые квадр. расширения: $k = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$, $\mathcal{O}_k = \mathbb{Z}[i]$. или
$k = \mathbb{Q}(\sqrt{-2})$, $\mathcal{O}_k = \mathbb{Z}[\sqrt{2}i]$. (см. п. 3)).

2 Алгебраические k-группы

Пусть $k \subset \mathbb{C}$ – поле хар. $\mathrm{char}(k) = 0$. Наши основные поля: $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, или поля алгебр. чисел.

Опр. Алгебр. подмн-е $X \subset \mathbb{C}^n$ – это мн-во решений сист. полиномиальных уравнений. Мн-ие X замкнуто над k, если эти $p_j \in \mathbb{C}[z_1, \dots, z_n]$ имеют коэф. из k, т.е. $p_j \in k[z_1, \dots, z_n]$. Для $\mathrm{char}(k) = 0$ это равносильно тому, что X опред. над k, т.е. идеал $\mathcal{J}(X) = \{p \in \mathbb{C}[\bar{z}] \mid p(\bar{z}) = 0 \ \forall \bar{z} \in X\}$ порожден многочленами над k. (Будем говорить, что X – k-многообр.)

Топология Зарисского: Замкнутые подмн-ва в k^n $\Leftrightarrow$ решения сист. полином. ур-й $\begin{cases} p_1(z) = 0 \\ \vdots \\ p_N(z) = 0 \end{cases}$
В частн., топология Зарисского на $X \subset k^n$ определяется алгеброй $k[X] = k[z_1 \dots z_n] / \mathcal{J}(X)$.
Топология Зарисского слабее обычной топологии в $\mathbb{R}^n$ или $\mathbb{C}^n$, а также топ. Зарисского в $k^{n+m} \neq$ топ. Зарисского на $k^n \times k^m$ (Пример $X = \{z_1 = z_2\}$).
Говорят, что $A \subset X$ плотно по Зарисскому в X, если $p(A) = 0 \Rightarrow p(X) = 0$.
Замыкание по З-му: $Z\mathrm{cl}(A)$. Напр., $\mathbb{Z}$ дискр. в $\mathbb{R}$, но $Z\mathrm{cl}(\mathbb{Z}) = \mathbb{R}$.

Пусть $X \subset \mathbb{C}^N$ – алг. мн-е. Тогда $X(k) = X \cap k^N$; $X(\mathcal{O}_k) = X \cap \mathcal{O}_k^N$.
рац. точки целые точки

Опр. Алгебраическая k-группа – это алг. k-мн-е G, которое явл. группой с групповыми операциями $\mu(x,y) = xy$ и $\tau(x) = x^{-1}$, которые сами являются полиномиальными k-морфизмами.

Теор. Всякая алг. $\mathbb{C}$-группа, связная в $\mathbb{R}$-топол., явл. связной в т. Зар. Верно и обратное: связная в т. Зар. $\mathbb{C}$-группа будет $\mathbb{C}(\mathbb{R})$-связной.

Контрпример для $\mathbb{R}$-групп: $G = \mathbb{R}^*$ – несвязна в $\mathbb{R}$-топологии.

Теор. Алгебр. K-группы при $K = \mathbb{R}$ и $K = \mathbb{C}$ являются группами Ли.

Опр. Пусть $x \in GL_n(\mathbb{C})$. Тогда $\exists!\, x_s, x_u \in GL_n(\mathbb{C})$:

$x = x_s x_u = x_u \cdot x_s$, где x_s – п/п элемент (диагонализуемый), x_u – унипотентный эл-т, т.е. $(x_u - 1)$ – нильп.: $(x_u - 1)^m = 0 \Leftrightarrow$ все $\lambda(x_u) = 1$.

k-Тор – коммут. алгебр. k-группа, связная и сост. из полупростых (диаг) элементов. Всякий тор сопряж. подгр. диаг. матриц и изоморфен $\underbrace{GL_1 \times \ldots \times GL_1}_{\dim T} = k^* \times \ldots \times k^*$. Тор назыв. k-расщепимым, если он k-изоморфен $(k^*)^{\dim T}$. Вещ. ранг гр. G – dim макс. $\mathbb{R}$-расщ. тора ($\mathrm{rank}_{\mathbb{R}} G$).

Примеры классических групп.

1) $GL_n(k) \subset \mathbb{C}^{n^2}$. Заметим, что $GL_n(k) \subset \mathbb{C}^{n^2+1}$ и задается уравнением $\det(z_{ij}) \cdot t = 1$. $\{z_{11}, \ldots, z_{nn}, t\}$

Очевидно, что $\mu: G \times G \to G$ – полин. морфизм, а взятие обратного выполняется так: $\tau(z) = z^{-1} = (w_{ij})$, где

$$w_{ij} = (-1)^{i+j} \cdot \frac{m_{ij}}{\det(z_{ij})} = (-1)^{i+j} m_{ij} \cdot t.$$

2) $G = SL_n(k) = \{\det(z) = 1\}$.

Заметим, что $\mathrm{rank}_{\mathbb{R}} SL_n(\mathbb{R}) = n-1$. Известно, $PSL_2(\mathbb{R}) \simeq SO^0_{2,1}(\mathbb{R})$, $PSL_2(\mathbb{C}) \simeq SO^0_{3,1}(\mathbb{R})$.

3) $G = SO_q(k)$, где $q = (q_{ij})$ – квадр. k-форма.

Напр., $q(x) = -x_0^2 + x_1^2 + \ldots + x_n^2$.

Тогда $SO_q(\mathbb{R}) \cong SO_{n,1}(\mathbb{R}) := \{A \in GL_{n+1}(\mathbb{R}) \mid A^T I_{n,1} A = I_{n,1}\}$, $I_{n,1} = \mathrm{diag}(-1,1,\ldots,1)$

Но $SO_q(\mathbb{C}) = SO_{n+1}(\mathbb{C})$.

4). Есть еще группы $SO_{p,q}$; $Sp_{m,n}$; $U_{m,n}$.

$\mathrm{rank}_{\mathbb{R}} SO_{p,q} = \mathrm{rank}_{\mathbb{R}} Sp_{p,q} = \min\{p,q\}$; $\mathrm{rank}_{\mathbb{R}} U_{n,1} = 1$.

④ Арифметические группы

Пусть $k \subset \mathbb{R}$ - вполне вещ поле алг. чисел, $\mathcal{O}_k$ - кольцо целых.

Пусть H - неком. п/п группа Ли, т.что H° не имеет комп. множ.

Опр. Алгебр. k-группа G назыв допустимой для H, если G — простая и $\exists$ сюр. гомом. $\varphi: G(k \otimes \mathbb{Q}) \to H$.

$\left(G(k\otimes\mathbb{Q}) = \prod_{\sigma: k \hookrightarrow \mathbb{R}} G^\sigma(\mathbb{R}) \right)$

Т.е. $\prod_\sigma G^\sigma(\mathbb{R}) \cong H \times K$.

Опр. $\Gamma_1, \Gamma_2 < H$ соизмеримы, если $[\Gamma_j ; \Gamma_1 \cap \Gamma_2] < +\infty$ $\forall j = 1,2$ $(\Gamma_1 \sim \Gamma_2)$.

Они соизм. в широком смысле, если $\exists h \in H : h\Gamma_1 h^{-1} \sim \Gamma_2$.

Теорема (Borel & Harish-Chandra '1962, Ann. Math.)

Если для $\Gamma < H$ верно, что $\Gamma \sim G(\mathcal{O}_k)$, где G - доп. k-гр. для H, то Γ - решетка в H (по мере Хаара).

Более того, если $\pi : G(k\otimes\mathbb{Q}) \to G(k\otimes\mathbb{Q})/K'$, где $K' < K$ (какая-то часть), $G(k\otimes\mathbb{Q}) \cong H \times K$,

то $\pi(G(\mathcal{O}_k))$ - решетка в $\pi(H \times K)$.

Опр. Решетки в H из теор. Б-Х-Ч наз. арифметическими.

Теор (Borel's Density Theorem).

Пусть $\Gamma < G$ - решетка в п/п гр-Ли без комп. множ. [вещ. алгебр. группе $G \subset GL_N(\mathbb{R})$]. Тогда $Zcl(\Gamma) = G$

т.е. если $p(x_{11}, \ldots, x_{nn}) \in \mathbb{R}[x_{11}, \ldots, x_{nn}]$ (многочлены на $Mat_N(\mathbb{R})$)

и $p(\Gamma) = 0$, то и $p(G) = 0$.

Замечание с прошлой лекции: Надо подправить.
1) $G \not\cong SL_2(\mathbb{R})\times K$
2) Mostow vs. Margulis

Теор (Margulis Superrigidity Theorem '19)

Пусть $G_1 \not\cong SO_{n,1}(\mathbb{R})\times K$ или $SU_{n,1}(\mathbb{R})\times K$ (изогения). ($\Leftarrow rk_{\mathbb{R}} G_1 \geq 2$).

Пусть G_1, G_2 - связные п/п гр. Ли без центра и компактных множителей.

Пусть $\Gamma < G_1$ неприводим. решетка и $\varphi : \Gamma \to G_2$ - гомоморфизм, т.что $Zd(\Gamma) = G_2$ (замыкание по Зарисскому). Тогда φ продолж. до непр. гомоморфизма $\hat{\varphi} : G_1 \to G_2$.

(Грубо говоря, $\Gamma_j < G_j$ реш., $\varphi : \Gamma_1 \xrightarrow[\text{гом}]{} \Gamma_2 \Rightarrow \exists \hat{\varphi} : G_1 \to G_2$)

Опр. Решетка $\Gamma < G$ неприв., если ΓN всюду плотна в G° для всякой некомп., замкн. норм. подгр $N \triangleleft G$.

Теор. (Strong Mostow Rigidity)

Пусть G_1, G_2 - связные п/п гр. Ли без центра и комп. множ., $G_1 \not\cong PSL_2(\mathbb{R})$, $\Gamma_j < G_j$ - неприв. решетки. Тогда всякий изоморфизм $\varphi : \Gamma_1 \xrightarrow{\sim} \Gamma_2$ продолж. до непр. изом. $\hat{\varphi} : G_1 \xrightarrow{\sim} G_2$.

Теор. (Маргулис)

Пусть $\Gamma < H$ - решетка, и пусть $Comm_H(\Gamma) = \{h \mid h\Gamma h^{-1} \sim \Gamma\}$

Тогда Γ - арифм. подгр $\Leftrightarrow Comm_H(\Gamma)$ плотен в H

Γ - неарифм. $\Leftrightarrow Comm_H(\Gamma) \sim \Gamma$, т.е. решетка.

(Ясно, что $Comm_H(\Gamma) \supset \Gamma$; и если Γ - арифм. т.е $\Gamma \sim G(\mathcal{O}_k)$, то $Comm_H(\Gamma) \supset G(k)$.)

Теор (Винберг '1971).

Пусть $\Gamma < G$ - дискр. подгр. в п/п компл. алг. гр., причем $Zd(\Gamma) = G$. Пусть $Ad : G \to GL(\mathfrak{g})$ - присоед. пр-ставление. Тогда adjoint trace field $k = \mathbb{Q}(\{tr(Ad\,\gamma) \mid \gamma \in \Gamma\})$ - инвариант класса соизм гр. Γ и $\Gamma < G(k)$. М.сл., что $\exists k$-гр. G' : $\Gamma < G'(k)$ и $G'(\mathbb{C}) = G$.

__Теор__ (Margulis Arithmeticity Theorem '1974).

Всякая непривод. решетка $\Gamma < G$ в п/п гр. Ли за исключением случая, когда G изогенна $SO_{n,1}(\mathbb{R}) \times K$ или $SU_{n,1} \times K$, явл. арифметической.