# خلاصه‌ای از سخنرانیهای پروفسور پرِگر در مرکز

## طرحهای بلوک‌ـانتقالی

یک $(v, k, \lambda)$ ـ $t$ طرح $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ متشکل است از یک مجموعهٔ $v$ نقطه‌ای $\mathcal{P}$ و یک گردایهٔ $\mathcal{B}$ از زیرمجموعه‌های $k$ عضوی $\mathcal{P}$ (که بلوک نامیده می‌شوند)، با این خاصیت که هر $t$ـزیرمجموعهٔ $\mathcal{P}$ دقیقاً در $\lambda$ بلوک ظاهر می‌شود. هر اتومورفیسمِ چنین طرحی، جایگشتی از $\mathcal{P}$ است که بلوک را به بلوک تبدیل می‌کند؛ از این رو مجموعهٔ تمامی اتومورفیسمها زیرگروهی از گروه متقارنِ $\mathrm{Sym}(\mathcal{P})$ تشکیل می‌دهد. اگر $\mathrm{Aut}(\mathcal{D})$ روی $\mathcal{B}$ انتقالی باشد، آنگاه طرحِ بلوک‌ـانتقالی نامیده می‌شود.

خانوادهٔ $t$ـطرحهای بلوک‌ـانتقالی خصوصیات زیادی از خود بروز می‌دهد که در خانواده‌های کلّیتری از طرحها دیده نمی‌شود. به‌عنوان مثال در $t$ـطرحهای بلوک‌ـانتقالی، به استثنای $t$ـطرحهای بدیهی که در آنها $\mathcal{B}$ شامل تمامیِ زیرمجموعه‌های $k$ عضوی است، باید $t \leq ۷$، و حدس زده می‌شود که $t$ حداکثر برابر با ۵ است (کَمِرن و پرِگر). به‌طورکلّی برای پی بردن به ساختمان طرحهای بلوک‌ـانتقالی و یافتنِ تدبیری برای جستجوی نمونه‌هایی از این‌گونه طرحها، زیرگروههای انتقالیِ $\mathrm{Sym}(\mathcal{P})$، و به‌خصوص زیرگروههای انتقالیِ ماکزیمال در $\mathrm{Sym}(\mathcal{P})$ نقش اساسی دارند. نتایج اخیر برای رسیدن به این هدف با تأکید خاصی بر طرحهای بلوک‌ـانتقالیِ غیراولیه روی نقاط مطرح گردید.

## شرایط متناهی بودن برای عمل گروه

در سال ۱۹۵۴ بی.اچ. نیومن، قضیه‌ای در بارهٔ پوشاندنِ یک گروه مجرد با تعدادی از همدسته‌های زیرگروههای سرهٔ آن ثابت کرد. در سال ۱۹۷۶ پی.ام. نیومن، نشان داد که این نتیجه با قضیه‌ای در بارهٔ جداسازیِ زیرمجموعه‌هایی از نقاط تحت عمل گروه معادل است. شرحی از این نتیجهٔ اساسی توسط برج، برتْز، مَک‌دانلد و نیومن ارائه شد (۱۹۷۶):

**قضیهٔ جداسازی.** *فرض کنید $G$ گروهی از جایگشتهای مجموعهٔ $\Omega$ باشد و فرض کنید $\Gamma$ و $\Delta$ زیرمجموعه‌های متناهی‌ای از $\Omega$ با اندازه‌های به‌ترتیب $m$ و $n$ باشند. اگر کلّیهٔ $G$ـمدارها دارای طولِ بزرگتر از $mn$ باشند، آنگاه عضوی مانند $g \in G$ وجود دارد که $\Gamma^g \cap \Delta = \varnothing$.*

در یک درسِ ۵ جلسه‌ای، شرحی بر این نتیجه و تعدادی از کاربردهای آن ارائه شد. به‌ویژه مفهوم حرکتِ یک زیرمجموعهٔ $\Gamma$ معرفی شد: اگر به ازای هر $g \in G$، $|\Gamma^g \backslash \Gamma|$ متناهی و کراندار باشد آنگاه حرکتِ $\Gamma$، $\mathrm{mov}(\Gamma)$، را برابرِ $\max\limits_{g \in G} |\Gamma^g \backslash \Gamma|$ تعریف می‌کنیم.

تعمیمی از قضیهٔ جداسازی نیز ثابت شد:

**قضیه (پرِگر).** *فرض کنید $G$ گروهی از جایگشتهای $\Omega$، و $\Gamma \subset \Omega$ زیرمجموعه‌ای از اندازهٔ $k$ باشد. اگر $mov(\Gamma) = m < k$، آنگاه حداقل یک $G$ـمدار با طولِ کوچکتر از $k^۲/(k-m)$ وجود دارد که اشتراکش با $\Gamma$ تهی نیست.*

نتایج دیگری در بارهٔ حرکتِ زیرمجموعه‌ها تحت عمل گروه نشان داده شد. به‌عنوان مثال، اگر $\mathrm{mov}(\Gamma) = m$، آنگاه $\Gamma$ دارای تفاضل متقارن با مجموعهٔ $G$ـپایداری از اندازهٔ حداکثر $۲em\lceil \ln(۲m) \rceil$ است (بریلَفسکی، بِسچِنیک و پرِگر). همچنین، اگر تمامی $k$ـزیرمجموعه‌ها به ازای $m < k$ دارای حرکتِ حداکثر $m$ باشند، آنگاه طول و تعداد $G$ـمدارهای غیربدیهی توسط تابعی خطّی از $m$ کراندار می‌شوند (پرِگر).

در خاتمه مسأله‌ای از گروههای مجرد (شرایط مربعات متناهی برای گروهها) و نتیجه‌ای از گروههای انتقالی با زیردرجهٔ کراندار مورد بحث قرار گرفت و به ارتباط آنها با قضیهٔ جداسازی اشاره شد.

# خلاصهٔ سخنرانی پروفسور موروزُف در سمینار فارابی

## محاسبه‌پذیری در ریاضیات

زمانی ریاضیدانِ برجستهٔ روس آ.د. تایمانُف گفته بود که در ریاضیاتِ باستان اساسیترین مسأله این بود که «ماهیت عدد چیست؟»، درحالی که در ریاضیاتِ امروزی مسأله این است: «چگونه می‌توان توابع را تعریف (محاسبه) نمود؟».

الگوریتمها هزاران سال است که شناخته شده‌اند. به‌عنوان مثال می‌توان از الگوریتم اقلیدسی برای پیدا کردنِ بزرگترین مقسوم‌علیه مشترکِ دو عددِ طبیعی، یا الگوریتمهای معمول ضرب و تقسیم که در مدارس آموخته می‌شوند نام برد.

الگوریتمها فرآیندهای خاصی هستند که کامپیوترها یا انسانها می‌توانند آنها را اجرا کنند. معمولاً هر الگوریتم شامل شرحِ کاملی است که توسط تعدادی متناهی کلمه داده می‌شود. هر الگوریتم مرحله به مرحله اجراء می‌گردد. هر مرحله از یک الگوریتم متشکل است از مجموعه‌ای از تغییراتِ مقدماتی بر روی خانواده‌ای متناهی از اطلاعات. در هر مرحله ما دقیقاً می‌دانیم که چه انجام دهیم و، اگر حافظه و وقت و کاغذ کافی موجود باشد، تمام مراحل را می‌توان اجرا کرد ـبه‌عنوان مثال، پیدا کردن کوچکترین عدد در میانِ $۱۰^{۱۰}$ عدد، همان میزانِ اجراشدنی است که محاسبهٔ تابع تالی.

برای نشان دادنِ وجودِ یک الگوریتم برای حلِ یک مسأله می‌توان تنها الگوریتم را توصیف کرد و ثابت کرد که مسأله را حل می‌کند، اما برای اثباتِ وجود نداشتنِ الگوریتمی برای یک مسأله به مفهوم ریاضیِ الگوریتم احتیاج

داریم. برای چنین مقصودی راههای زیادی توسط افراد مختلف ارائه شده است. در حقیقت صورتبندیِ کاملی از الگوریتم وجود ندارد ولی توصیفاتِ قابل قبولی از توابع محاسبه‌پذیر وجود دارد: توابع جزئیِ بازگشتی (چرچ، کلی‌نی، گودل)، ماشینهای تیورینگ، ماشینِ پست، ماشینِ شونفیلد، توابعِ Σ-تعریف‌پذیر روی اعداد طبیعی، و غیره. اینها بر شهودهای مختلف در مورد محاسبه‌پذیری متکی هستند و البته ثابت شده است که همهٔ این مفاهیمْ یک ردهٔ واحد از توابع محاسبه‌پذیر را مشخص می‌کنند.

این نتیجهٔ روش‌شناختی به تزِ چرچ معروف است: هر تابعْ به‌طور شهودی محاسبه‌پذیر است اگر و تنها اگر جزئیِ بازگشتی باشد. این تز را نمی‌توان به‌طور ریاضی ثابت نمود چرا که حکم ریاضی‌ای نیست و تنها تجربهٔ ریاضی است که این حکم را ثابت می‌نماید.

با استفاده صورتبندیِ بالا و تزِ چرچ ثابت شده است که بعضی از مسائل به‌طور الگوریتمی تصمیم‌ناپذیرند. برای مثال، ممکن نیست که بتوان الگوریتمی ساخت که مشخص کند که حکم ریاضیِ داده شده‌ای (در زبانی به اندازهٔ کافیِ غنی مانند فارسی) درست یا نادرست است؛ گروه متناهیاً نمایش‌پذیری وجود دارد که مسألهٔ واژهٔ آن تصمیم‌ناپذیر است (آدیان، نوویکف)؛ الگوریتمی برای پیدا کردن ریشه‌های صحیح چندجمله‌ایِ با ضرایب صحیحِ داده شده‌ای وجود ندارد (ماتیاسویچ).

الگوریتم مفهومی کاملاً بنیادی است. کدام‌یک اول به‌وجود آمد: عدد یا الگوریتم؟ این چندان واضح نیست. برای اجرای یک الگوریتم به اعداد طبیعی احتیاج داریم؛ از این رو به‌نظر می‌رسد الگوریتمها منشعب از اعداد باشند. از طرف دیگر برای تولید اعداد طبیعی به شمارش احتیاج داریم: ۱، ۲، ۳، . . .، که شبیه یک الگوریتم است. علاوه بر آن ما در ذهن قادر به نمایش اعداد بزرگی چون ۲۵، ۶۴، $10^{10}$ بدون اِعمالِ الگوریتمی یا نوعی تعریف یا ساخت نیستیم؛ یعنی ما می‌توانیم اعدادی مانند ۰، ۱، ۲، . . . را درک کنیم، با این حال برای نمایش عدد ۲۵ چیزی شبیه این خواهیم گفت: «۵ سطر را در نظر بگیرید که در هر سطرِ آن ۵ نقطه وجود داشته باشد»، یا برای نمایشِ ۶۴ از چیزی شبیهِ «تعداد مربعهای صفحهٔ شطرنج» استفاده می‌کنیم.

در مطالعهٔ محاسبه‌پذیری دوگرایشِ عمده وجود دارد: افزودنِ محاسبه‌پذیری به ساختارهای کلاسیکِ ریاضیات، و کاربرد مفاهیم کلاسیک برای درک محاسبه‌پذیری. بعضی از شاخه‌های ریاضیات که با محاسبه‌پذیری سر و کار دارند اینها هستند: آنالیز ریاضیِ ساختنی، فضاهای توپولوژیکِ محاسبه‌پذیر، دامنه‌های اسکات، جبرها و مدلهای ساختنی، و بالاخره بعضی از بخشهای منطق مانندِ درجاتِ حل‌ناپذیری، محاسبه‌پذیری در دامنه‌های مجرد (ماشینهای مجرد، تعریف‌پذیری با انواعِ مختلفِ فرمولها)، تصمیم‌پذیریِ تئوریها و غیره.

اگر نظرمان را در مورد قدمهای ابتدایی الگوریتم تغییر دهیم، یعنی انواعِ دیگری از قدمها را ابتدایی در نظر بگیریم (مثلاً اگر بتوانیم در هر مرحله یک مسألهٔ به‌طور الگوریتمیْ تصمیم‌ناپذیر را حل کنیم)، آنگاه وارد مفاهیم دیگری از محاسبه‌پذیری می‌شویم که بسیاری از خواصِ مفهومِ قبلی را دارند. بنابراین می‌توانیم مفهومِ محاسبه‌پذیری را «فازی»تر سازیم. می‌توانیم انواعِ محاسبه‌پذیری را به‌عنوان گونه‌های مختلفِ تعریف‌پذیری (با رده‌های مختلفی از فرمولها) تلقی کنیم.

محاسبه‌پذیری یکی از اساسیترین مفاهیم در ریاضیات است که در تمام قسمتهای آن ریشه دوانده است. این مفهوم، عمل یا ساختار را به خانوادهٔ اشیاء بنیادی‌ای که در ریاضیات بررسی می‌شوند می‌افزاید. محاسبه‌پذیری در حقیقت بخشی از مفهومِ تعریف‌پذیری است.