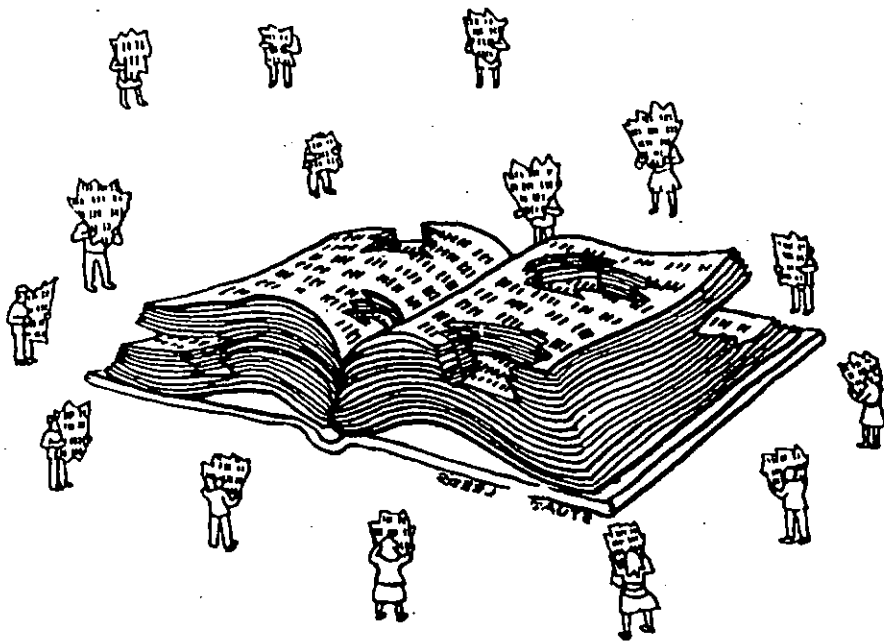


# ریاضیات معاصر

## گشت و گذاری در



مقدمه: آغاز هزارهٔ سوم و ابتدای قرن بیست و یکم میلادی، یعنی، سال ۲۰۰۰، برابر با یازدهم دیماه ۱۳۷۸ تا دهم دیماه ۱۳۷۹ را سال جهانی ریاضیات نام نهاده‌اند، و این اهمیت ریاضیات را در دنیایی که با هزارهٔ سوم آغاز می‌شود نشان می‌دهد، ریاضیاتی که هدف ساختن نه تنها رایانه‌های هرچه پیشرفته‌تر را دارد که بر سر ابداع ماشینهای متفکر است و از قعر گل سیاه تا اوج زحل را در نور دیده.

مقاله‌هایی که از این شماره به بعد، تحت عنوان گشت و گذاری در ریاضیات معاصر منتشر می‌شود، با توجه به این نقش حیاتی ریاضیات در زندگی انسانها، و به توصیهٔ هیأت تحریریهٔ مجلهٔ برهان و برای آشنایی هرچه بیشتر خوانندگان این مجله، تهیه و تنظیم شده‌اند. مقاله‌ها به سفارش هیأت تحریریهٔ مجله، کوتاه؛ اما بسیار دقیق هستند و آشنایی مختصری به خوانندهٔ علاقه‌مند به ریاضیات می‌دهند و مطالب آنها با استفاده از دایرة المعارف فشردهٔ ریاضیات نوشتهٔ ریاضیدانهای آلمانی تهیه و تنظیم شده‌اند.

\*\*\*

### رمزگذاری

از دوران باستان تا عصر حاضر، پیامهای سری بسیاری ارسال شده است، و نیاز به ارتباطهای مخفیانه، به طور سنتی، در موارد

سیاسی و نظامی بسیاری رخ داده است.

\* امروزه، مسألهٔ پیامهای سری، با به میان آمدن کاربردهای وسیعی از ارتباطهای الکترونیکی، حتی در مورد مذاکرات مالی نیز ضروری شده است. در نتیجهٔ علاقهٔ بسیاری به روشهایی وجود دارد که پیامها را برای هر کس، غیر از دریافت کنندهٔ مورد نظر نامفهوم کند.

یکی از دستگاه‌های رمزی، مبتنی بر مسألهٔ پشت‌واره است، صورت این مسأله چنین است:

\* با معلوم بودن مجموعه اعداد صحیح و مثبت  $a_1$  تا  $a_n$ ، و عدد صحیح  $S$ ، مشخص کنید که کدامیک از عددهای مزبور، با جمع شدن با یکدیگر،  $S$  را به دست می‌دهند.

رایانه کاران نشان داده‌اند که رمزهای پشت‌واره‌ای، برای رمزنگاری کلید همگانی رضایت‌بخش نیستند.

\*\*\*

### مجموعه‌های هم توان

دو مجموعهٔ  $S$  و  $T$  را هم توان گویند اگر نگاشت دوسویی از  $S$  به  $T$  موجود باشد. عدد اصلی، رده‌ای از مجموعه‌های هم توان با مجموعه‌ای مفروض است. اعداد اصلی مجموعه‌های متناهی به اعداد طبیعی موسومند، و اعداد اصلی مجموعه‌های نامتناهی را

ترامتهای می‌نامیم.

\* در این صورت، و با توجه به تعاریف مربوطه، نمی‌توان با خانوادهٔ جمیع مجموعه‌ها، یا حتی با خانوادهٔ جمیع مجموعه‌های هم‌توان با مجموعه‌ای مفروض سر و کار داشت؛ زیرا این کار به پارادوکس راسل منجر می‌شود.

\* برای اجتناب از این وضع، معمولاً تعریف مربوطه را به خانوادهٔ  $F$  محدود می‌کنیم که حتی‌الامکان بزرگ و ضروری باشد.

در این حالت، اعداد اصلی، خود مجموعه یعنی، خانوادهٔ مجموعه‌ها هستند، گرچه ممکن است بعدها گسترش دادن خانوادهٔ  $F$  ضروری شود.

\*\*\*

\* عنصر دلخواه  $a$  را از  $S$  اختیار می‌کنیم، سپس عنصر دومی، و همین‌طور الی آخر. اگر  $S$  نامتناهی باشد، دنبالهٔ

$a_0, a_1, \dots$

را به دست می‌آوریم. اکنون یا  $S$  به اتمام رسیده است یا نه؛ اگر نه، فرآیند مزبور را تا زمانی که برای به اتمام رسیدن مجموعهٔ مورد بحث، لازم است ادامه می‌دهیم.

\* اگر  $S$  توسط دنباله‌ای که عناصر مورد بحث در آن انتخاب شده‌اند مرتب شده باشد، در این صورت، هر زیر مجموعه دارای یک کوچکترین عنصر است؛ یعنی عنصری که ابتدا انتخاب شده است.

\*\*\*

### منطق ریاضی

یکی از کارهای اصلی منطق ریاضی، بررسی تفکر صوری و استنتاج به کمک روشهای ریاضی مثلاً گرفته شده از جبر یا نظریهٔ الگوریتمهاست.

\* اما این کار، که آغاز در فلسفه دارد، تنها کار آن نیست؛ امروزه منطق ریاضی، شامل انبوهی موضوعات و کاربردها در حوزه‌های بسیار گوناگونی از قبیل علوم طبیعی، جبرگژینشی، نظریهٔ دستگاه‌های پردازش داده‌ها، زبانشناسی، چندین شاخه از علوم اجتماعی چون فلسفه، حقوق، و اخلاق است.

\* انگیزهٔ قطعی در توسعهٔ منطق ریاضی، از وضعیت ریاضیات در پایان قرن نوزدهم به وجود آمد. تا آن زمان، ریاضیات تعداد فراوانی از دستاوردهای جداگانه را جمع کرده، به درجهٔ بالایی از تجرید رسیده بود، بدون این که به وضوحی متناسب با آن مورد محتوای مفاهیم اساسی‌ای نائل شده باشد که به شیوه‌ای شهودی، مثلاً مفهوم مجموعه یا مفهوم استنتاج منطقی، به کار رفته بودند. در آن زمان، غیر از نیاز به بنیان غیر قابل تردیدی برای مفهوم مجموعه، برای اولین بار دریافت معنای درست منطق و قیاس منطقی، ضروری شد.

\*\*\*

### فرض پیوستار

فرض پیوستار، بر این است که مجموعه‌ای نامتناهی از اعداد حقیقی یا شماراست یا عدد اصلی  $N$  را داراست.

در ۱۹۶۴ کوهن ثابت کرد که، اثبات فرض پیوستار، با استفاده از اصول موضوع مجموعه - نظری استاندارد، غیرممکن است. \* پیش از این، در ۱۹۳۸، گودل نشان داده بود که فرض پیوستار این اصول موضوع را نقض نمی‌کند.

این دو نتیجه، با هم نشان می‌دهند که فرض پیوستار از سایر اصول موضوع مجموعه - نظری مستقل است.

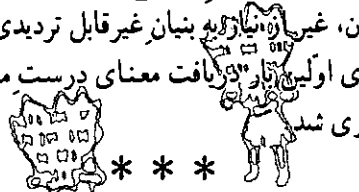
\* اما خود پیوستار چیست؟ طبق تعریف، عدد اصلی مجموعهٔ اعداد حقیقی به عدد اصلی پیوستار موسوم است و با  $N$  یا  $C$  نمایش داده می‌شود.

عدد اصلی مجموعهٔ اعداد حقیقی، در بازهٔ باز  $(0, 1)$  نیز  $N$  است؛ زیرا این بازه به طور دوسویی به مجموعهٔ جمیع اعداد حقیقی نگاشت می‌یابد.

\*\*\*

### قضیهٔ خوش‌ترتیبی

یکی از قضایای نظریهٔ مجموعه‌ها، قضیهٔ خوش‌ترتیبی است. این قضیه چنین است: بر هر مجموعهٔ  $S$  رابطه‌ای موجود است که تحت آن  $S$  خوش‌ترتیب است. کاتوره این قضیه را به عنوان یکی از اصول تفکر در نظر گرفته، آن را به ترتیبی که خواهیم گفت معقول کرده بود، این ترتیب چنین است:



### اصولهای منطق گزاره‌ها

گزاره‌ها، نامی است که در مورد ساختارهای زبانی معینی، برای توصیف و انتقال اطلاعات، به کار می‌رود. منطق گزاره‌های کلاسیک، با فرض آغاز می‌شود. دنبالهٔ اصل دو ارزشی، هر گزاره، یا راست یا دروغ است.



صورت‌های خاص، استفاده مکرر از متغیرها و نمادهای مخصوص توابع یا رابطه‌هاست.

\* متغیرها، نمادهای از پیش تخصیص یافته‌ای هستند که اشیای دلخواه حوزه‌ای قبلاً مشخص شده را نمایش می‌دهند. نمادهایی از قبیل  $+$  و  $o$ ، در حوزه اعداد طبیعی، که معنایشان معین است، به ثابت‌ها موسوم‌اند.

ویژگی دیگر زبان ریاضی، امکان متغیرهای مقید، به کمک سورهای منطق محمولی است.

\* در عبارت «اعداد  $p$  و  $q$  ای چنان وجود دارند که  $2n = p + q$ » نمادهای  $p$  و  $q$  توسط تابعگون محمولی - منطقی «وجود دارد» مقید شده‌اند، در حالی که متغیر  $n$  آزاد است.

آشکار شده که برای کاربردهای متغیرهای مقید در ریاضیات، دو عمل منطق محمولی «وجود دارد» و «به ازای هر» کافی‌اند. بنابراین زبانهای منطق محمولی تنها مبتنی بر این نوع متغیرهای مقیدند.

\* \* \*

## زبانهای محمولی و الگوریتمی

زبانهای منطق محمولی توصیفی‌اند؛ یعنی عبارتهای چنین زبانهایی روابط رایج در ساختارهای ریاضی را توصیف می‌کنند. زبانهای الگوریتمی، با توسعه پردازش داده‌ها توسط ماشینها، اهمیت یافته‌اند. زبانهای الگوریتمی، دارای کاربرد فرمان دادن، راه انداختن عملیات و هدایت کردن فرایندها هستند. مثالهایی از زبانهای الگوریتمی به کار رفته در تکنولوژی برنامه‌ریزی عبارتند از: COBOL، FORTRAN، PL1 و غیره.

\* حتی در زبانهای مقدماتی نیز بعضی عناصر الگوریتمی وارد شده‌اند: یک جمله را می‌توان به صورت دنباله‌ای از فرمانهایی در نظر گرفت که باید انجام گیرند؛ به عنوان مثال،  $(x+1).y$  نمایشگر این دنباله است:

« $1$  را با  $x$  جمع کن، آن گاه نتیجه را در  $y$  ضرب کن.»

\* اما ظهور الگوریتمها، در چهارچوب ریاضیات و منطق، به صورت روشهایی عمومی برای حل جمیع مسائل رده‌ای مفروض، انجام گرفته است.

\* \* \*

## الگوریتم و توابع بازگشتی

مفهوم دقیق الگوریتم، شرطی لازم، برای تحقیق این پرسش

مفهوم راستی یا صدق به کار رفته در این جا، که به ارسطو بازمی‌گردد، گزاره را در صورتی راست در نظر می‌گیرد که اظهار بیان شده با آن متناظر با حقیقتی باشد.

\* اصل دو ارزش مورد بحث، در واقع دربرگیرنده دو اصل زیر است: اصل اول، اصل طرد اوسط است که به موجب آن، هر گزاره راست یا دروغ است. اصل دوم، اصل طرد تناقض است که بنا بر آن، گزاره‌ای وجود ندارد که هم راست، هم دروغ باشد. \* بنابراین، رده جمیع گزاره‌ها به دو زیر رده مجزا تقسیم می‌شود، که با نمادهای  $1$  یا راست و  $0$  یا دروغ نمایش داده و ارزش راستی نامیده می‌شوند، ارزشهای راستی مزبور را با  $F$  و  $T$  نیز نمایش می‌دهند.

\* \* \*

## رابطهای منطق گزاره‌ها

گزاره‌های منطق کلاسیک را می‌توان به کمک ادوات زبانی‌ای از قبیل نه، و، یا، و غیره به گزاره‌های پیچیده‌تر ترکیب کرد.

\* بنا به دو مین اصل اساسی، یعنی اصل توسیع، ارزش راستی یک گزاره مرکب، منحصرأ توسط ارزشهای راستی مؤلفه‌های آن معین می‌شود و به معنای آنها بستگی ندارد.

در نتیجه، چنین ترکیباتی را می‌توان به صورت توابعی در نظر گرفت که ارزشهای راستی را به  $n$  تایی‌های ارزشهای راستی، تخصیص می‌دهند.

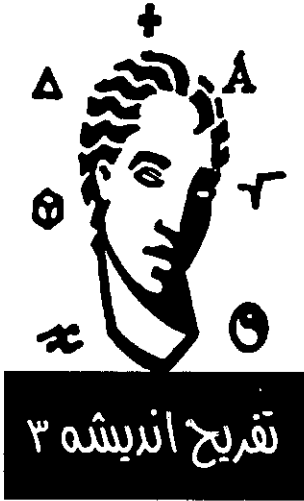
\* ادوات رابطی اغلب به کار رفته در منطق گزاره‌ها، متناظر با توابع ارزش نه، متناظر با ادوات نه، تابع ارزش و، متناظر با ادوات و، تابع ارزش یا، متناظر با ادوات یا، تابع ارزش اگر ... آنگاه ... متناظر با همین ادوات و تابع ارزش اگر و تنها اگر، متناظر با ادوات اگر و تنها اگر است.

کار منطق گزاره‌ها عبارت است از: تحلیل ریاضی این مفاهیم، که برای این منظور در چهارچوب حساسی به نام حساب گزاره‌ها، فرمول بندی می‌شوند.

\* \* \*

## منطق و زبان ریاضی

عبارتهای حساب گزاره‌ها برای تنظیم حقایق رخ دهنده در ریاضیات کافی نیستند؛ ترجمه فرمول بندی شده‌ای از زبان ریاضی، باید به طور قابل ملاحظه‌ای غنی تر باشد. در این مورد یکی از



۲	۲	۲	۲	=	۰
۲	۲	۲	۲	=	۱
۲	۲	۲	۲	=	۲
۲	۲	۲	۲	=	۳
۲	۲	۲	۲	=	۴
۲	۲	۲	۲	=	۵
۲	۲	۲	۲	=	۶
۲	۲	۲	۲	=	۱۰
۲	۲	۲	۲	=	۱۲

در هر سطر، بین ارقام ۲ علامتهای +، -، ×، : و ( ) را طوری قرار دهید که یک تساوی به دست آید.

● از کتاب تفریح اندیشه با بازیهای عددی ترجمه سیمین دخت ترکیور  
جواب در صفحه ۸۸

است که آیا مسائل خاصی از لحاظ الگوریتمی حل پذیرند یا خیر؟  
برسشهایی چنین حتی در قرون وسطی نیز مورد بحث بودند.

\* به عنوان مثال، حدود ۱۳۰۰ میلادی، ریمنودوس لولوس «Raymundus Lullus» اصطلاح ایده را مطرح کرد که مقصود از آن روشی عمومی برای یافتن جمیع حقایق ممکن بود. ایده های مزبور زمانی به اولین اوجشان رسیدند که لایب نیتس دریافت که مفهوم دقیق ایده شامل دو مفهوم تشخیص و تولید است.

\* این اندیشه بعد از لایب نیتس دنبال نشد. یکی از دلایل این دنبال نشدن آن بود که هنوز روشهای صوری کردن و تعبیر نمودن منطق ریاضی، که برای چنین برسشهایی ضروری اند، وجود نداشتند.

در حال حاضر، می توان به کمک توابع بازگشتی، صورت دقیق تشخیص و روش تولید را به دست داد. این مفاهیم، ابتدا برای مجموعه های اعداد طبیعی تعریف شدند.

\* \* \*

