



دانشگاه ساه نور

جبر

(رشته ریاضی)

دکتر سعادۃ اله فرامرزی

امروزه کتاب‌خوانی و علم‌آموزی، نه تنها یک وظیفه‌ی ملی، که یک واجب دینی است.

مقام معظم رهبری

در عصر حاضر یکی از شاخصه‌های ارزیابی رشد، توسعه و پیشرفت فرهنگی هر کشوری میزان تولید کتاب، مطالعه و کتاب‌خوانی مردم آن مرز و بوم است. ایران اسلامی نیز از دیرباز تاکنون با داشتن تمدنی چند هزارساله و مراکز متعدد علمی، فرهنگی، کتابخانه‌های معتبر، علما و دانشمندان بزرگ با آثار ارزشمند تاریخی، سرآمد دولت‌ها و ملت‌های دیگر بوده و در عرصه‌ی فرهنگ و تمدن جهانی به‌سان خورشیدی تابناک همچنان می‌درخشد و با فرزندان نیک‌نهاد خویش هنرنمایی می‌کند. چه کسی است که در دنیا با دانشمندان فرزانه و نام‌آور ایرانی همچون ابوعلی سینا، ابوریحان بیرونی، فارابی، خوارزمی و ... همچنین شاعران برجسته‌ای نظیر فردوسی، سعدی، مولوی، حافظ و ... آشنا نباشد و در مقابل عظمت آنها سر تعظیم فرود نیاورد. تمامی این افتخارات ارزشمند، برگرفته از میزان عشق و علاقه فراوان ملت ما به فراگیری علم و دانش از طریق خواندن و مطالعه منابع و کتاب‌های گوناگون است. به شکرانه‌ی الهی، تاریخ و گذشته ما، همیشه درخشان و پربار است. ولی اکنون در این زمینه در چه جایگاهی قرار داریم؟ آمار و ارقام ارائه‌شده از سوی مجامع و سازمان‌های فرهنگی در مورد سرانه‌ی مطالعه‌ی هر ایرانی، برایمان چندان امیدوارکننده نمی‌باشد و رهبر معظم انقلاب اسلامی نیز از این وضعیت بارها اظهار گله و ناخشنودی نموده‌اند.

کتاب، دروازه‌ای به سوی گستره‌ی دانش و معرفت است و کتاب خوب، یکی از بهترین ابزارهای کمال بشری است. همه‌ی دستاوردهای بشر در سراسر عمر جهان تا آنجا که قابل کتابت بوده است، در میان دست‌نوشته‌هایی است که انسان‌ها پدید آورده و می‌آورند. در این مجموعه‌ی بی‌نظیر، تعالیم الهی، درس‌های پیامبران به بشر، و همچنین علوم مختلفی است که سعادت بشر بدون آگاهی از آنها امکان‌پذیر نیست. کسی که با دنیای زیبا و زندگی‌بخش کتاب ارتباط ندارد بی‌شک از مهم‌ترین دستاوردهای انسانی و نیز از بیشترین معارف الهی و بشری محروم است. با این دیدگاه، به‌روشنی می‌توان ارزش و مفهوم رمزی عمیق در این حقیقت تاریخی را دریافت که اولین خطاب خداوند متعال به پیامبر گرامی اسلام (ص) این است که «بخوان!» و در اولین

سوره‌ای که بر آن فرستاده‌ی عظیم‌الشان خداوند، فرود آمده، نام «قلم» به تجلیل یاد شده‌است: «اقْرَأْ وَ رَبُّكَ الْأَكْرَمُ. الَّذِي عَلَّمَ بِالْقَلَمِ» در اهمیت عنصر کتاب برای تکامل جامعه‌ی انسانی، همین بس که تمامی ادیان آسمانی و رجال بزرگ تاریخ بشری، از طریق کتاب جاودانه مانده‌اند.

دانشگاه پیام‌نور با گستره‌ی جغرافیایی ایران‌شمول خود با هدف آموزش برای همه، همه‌جا و همه‌وقت، به‌عنوان دانشگاهی کتاب‌محور در نظام آموزش عالی کشورمان، افتخار دارد جایگاه اندیشه‌سازی و خردورزی بخش عظیمی از جوانان جویای علم این مرز و بوم باشد. تلاش فراوانی در ایام طولانی فعالیت این دانشگاه انجام پذیرفته تا با بهره‌گیری از تجربه‌های گرانقدر استادان و صاحب‌نظران برجسته کشورمان، کتاب‌ها و منابع آموزشی درسی شاخص و خودآموز تولید شود. در آینده هم، این مهم با هدف ارتقای سطح علمی، روزآمدی و توجه بیشتر به نیازهای مخاطبان دانشگاه پیام‌نور با جدیت ادامه خواهد داشت. به‌طور قطع استفاده از نظرات استادان، صاحب‌نظران و دانشجویان محترم، ما را در انجام این وظیفه‌ی مهم و خطیر یاری‌رسان خواهد بود. پیشاپیش از تمامی عزیزانی که با نقد، تصحیح و پیشنهادهای خود ما را در انجام این وظیفه‌ی خطیر یاری می‌رسانند، سپاسگزاری می‌نماییم. لازم است از تمامی اندیشمندانی که تاکنون دانشگاه پیام‌نور را منزلگاه اندیشه‌سازی خود دانسته و ما را در تولید کتاب و محتوای آموزشی درسی یاری نموده‌اند، صمیمانه قدردانی گردد. موفقیت و بهروزی تمامی دانشجویان و دانش‌پژوهان عزیز آرزوی همیشگی ما است.

دانشگاه پیام‌نور

فهرست مطالب

پیش گفتار	هفت
فصل اول	گروه‌های حل پذیر
۱-۱	مروری بر نظریه گروه‌ها ۱
۲-۱	سری گروه‌ها ۱۲
۳-۱	قضیه ژردان-هلدر ۱۸
۴-۱	گروه‌های حل پذیر ۲۱
۵-۱	مسائل حل شده فصل ۲۹
۶-۱	سؤالات چهار گزینه‌ای ۳۵
فصل دوم	حلقه‌های چندجمله‌ای
۱-۲	یادآوری حلقه‌ها ۴۱
۲-۲	حلقه چندجمله‌ای‌ها ۴۷
۳-۲	تجزیه در دامنه صحیح ۵۷
۴-۲	دامنه ایده‌آل اصلی (PID) ۶۳
۵-۲	دامنه تجزیه یکتا (UFD) ۶۷
۶-۲	محتوای یک چندجمله‌ای و چندجمله‌ای اولیه ۷۱
۷-۲	دامنه تجزیه یکتا بودن حلقه چندجمله‌ای‌ها ۷۹
۸-۲	تحویل ناپذیری یک چندجمله‌ای ۸۳
۹-۲	مسائل حل شده فصل دوم ۸۸
۱۰-۲	تمرین ۹۶

فصل سوم	توسیع میدان‌ها	۹۷
۱-۳	مروری بر فضاهاى بردارى	۹۸
۲-۳	توسیع میدان	۱۰۲
۳-۳	ریشه چندجمله‌ای‌ها	۱۰۴
۴-۳	توسیع جبرى	۱۰۷
۵-۳	میدان کرونگر	۱۰۹
۶-۳	میدان الحاقى	۱۱۳
۷-۳	یکریختى میدان الحاقى و کرونگر	۱۱۸
۸-۳	ریشه‌هاى چندگانه	۱۲۰
۹-۳	میدان شکافنده	۱۲۲
۱۰-۳	بستار جبرى	۱۳۱
۱۱-۳	مسائل حل شده	۱۳۷
۱۲-۳	تمرین	۱۴۳

فصل چهارم	قضیه بنیادی گالوا	۱۴۵
۱-۴	توسیع نرمال	۱۴۷
۲-۴	مشتق چندجمله‌ای‌ها	۱۵۳
۳-۴	توسیع جداپذیر	۱۵۶
۴-۴	میدان‌هاى متناهى	۱۶۴
۵-۴	قضیه بنیادی گالوا	۱۶۷
۶-۴	مسائل حل شده	۱۷۹
۷-۴	تمرین	۱۹۱

فصل پنجم	ترسیم‌پذیری	۱۹۳
۱-۵	ترسیم‌پذیری اعداد	۱۹۵
۲-۵	مضاعف کردن مکعب و تربیع دایره	۲۰۱
۳-۵	تثلیث زاویه	۲۰۲
۴-۵	ترسیم چندضلعی‌هاى منتظم	۲۰۵

۵-۵ سؤالات چهار گزینه‌ای ۲۱۶

فصل ششم پیوست ۲۱۹

۱-۶ ریاضی‌دانان نامی ایران ۲۲۰

۲-۶ ریاضی‌دانان برجسته غیر ایرانی ۲۲۷

واژه‌نامه انگلیسی - فارسی ۲۳۷

کتاب‌نامه ۲۵۳

تقدیم به فرزندانم:

پوریا

و

بردیا

پیش‌گفتار مؤلف

کتاب حاضر بر اساس مجوز شورای محترم تخصصی گروه ریاضی و شورای محترم تدوین دانشگاه پیام نور مطابق با آخرین سرفصل‌های درس جبر در رشته ریاضیات و کاربردها که مصوب وزارت علوم و تحقیقات و فناوری است تهیه و تنظیم شده است. این کتاب پنج فصل اصلی و یک فصل پیوست دارد. در انتهای هر فصل مسائل نمونه به همراه حل آنها آورده می‌شود که برای جمع‌بندی و مرور آن فصل تمرین‌های مناسبی هستند. علاوه بر این، مطالب و مثال‌هایی که در این مسائل بیان می‌شود به فهم بهتر و دقیق‌تر آن فصل کمک می‌کند و خلاء ناشی از کمبود مثال در متن فصل را جبران می‌کند.

فصل اول شامل ۴ بخش است. در بخش اول مقدماتی از نظریه گروه‌ها بیان می‌شود. در بخش دوم مفاهیمی مانند سری‌های نرمال، زیرنرمال و ترکیبی به صورت دقیق و کامل بررسی می‌شوند. مهم‌ترین قضیه این بخش، وجود یک سری ترکیبی برای هر گروه متناهی است. در بخش سوم هم‌ارزی نظریه‌های دو سری زیرنرمال بررسی می‌شود. مهم‌ترین قضیه این بخش، قضیه ژردان^۱ - هلدنر^۲ است که در آن هم‌ارزی دو سری ترکیبی (در صورت وجود) ثابت می‌شود. در بخش چهارم سری‌های حل‌پذیر و متعاقب آن گروه حل‌پذیر که نقش اساسی در نظریه گالوا دارند، معرفی و به طور کامل بررسی می‌شوند. سپس سری مشتق یک گروه تعریف و ارتباط آن با گروه حل‌پذیر بیان می‌شود. به بیان دقیق‌تر نشان داده می‌شود که شرط لازم و کافی برای حل‌پذیری یک گروه آن است که سری مشتق آن متناهی باشد. همچنین حل‌پذیری یک گروه با حل‌پذیری سری ترکیبی آن مقایسه می‌شود. مهم‌ترین نتیجه

1. C. Jordan

2. O. Holder

این بخش، اثبات حل پذیری گروه های متقارن S_n برای $n \geq 5$ است.

مطالب فصل دوم در ۸ بخش تنظیم شده است. در بخش اول با مروری اجمالی بر نظریه حلقه ها، قضایا و تعاریف اولیه لازم بدون برهان بیان می شود. در بخش دوم حلقه چندجمله ای ها معرفی و خواص آن بررسی می شود. مهم ترین قضیه این بخش، قضیه تقسیم است. در قضیه تقسیم، همانند آنچه در تقسیم اعداد رخ می دهد، تقسیم دو عضو حلقه چندجمله ای ها بر هم بررسی می شود. بخش سوم به بررسی مفاهیم اولیه خاصیت تجزیه در یک دامنه صحیح محدود می شود. به منظور بررسی این مهم در یک دامنه صحیح، مفاهیمی مانند عنصر اول و عنصر تحویل ناپذیر معرفی می شود. مهم ترین قضیه این بخش ارتباط بین عناصر اول و تحویل ناپذیر یک دامنه صحیح را بررسی می کند. در بخش چهارم دامنه های ایده آل اصلی بررسی می شود که در این نوع حلقه ها همه ایده آل ها اصلی هستند. این حلقه ها را به اختصار PID می نامیم. یکی از خواص مهم این حلقه ها این است که در این حلقه ها مفاهیم عنصر اول و عنصر تحویل ناپذیر یکسان هستند. مهم ترین قضیه این بخش این است که حلقه چندجمله ای ها با ضرایب در یک میدان، یک PID است. در بخش پنجم، دامنه های تجزیه یکتا بررسی می شوند. همان طور که در حلقه اعداد صحیح هر عدد صحیح به طور منحصر به فرد به حاصل ضربی از تعداد متناهی اعداد اول تجزیه می شود، این خاصیت تجزیه به برخی از دامنه های صحیح نیز تسری پیدا می کند. این حلقه ها را به اختصار UFD می نامیم. در مهم ترین قضیه این بخش نشان داده می شود که هر حلقه PID یک UFD است. یکی دیگر از نتایج ارزنده این بخش این است که حلقه چندجمله ای ها با ضرایب در یک میدان، یک UFD است. در بخش ششم، محتوی یک چندجمله ای معرفی می شود. به کمک این مفهوم تحویل ناپذیری یک چندجمله ای در دامنه تجزیه یکتا با تحویل ناپذیری آن چندجمله ای در میدان کسرهاش مقایسه می شود. در بخش هفتم، نشان داده می شود که خاصیت تجزیه یکتا از یک حلقه، به حلقه چندجمله ای هایش تسری می یابد. این بخش به بررسی تحویل ناپذیری یک چندجمله ای محدود می شود. مهم ترین قضیه این بخش، محک ایزنشتاین^۱ است که معیاری برای تحویل ناپذیری یک چندجمله ای است.

فصل سوم، شامل ده بخش است. بخش اول مروری بر مفاهیم اولیه و قضایای فضاهای

1. Eisenstein

برداری است. در بخش دوم و سوم توسیع یک میدان معرفی و مطالبی دربارهٔ ریشه‌های یک چندجمله‌ای بیان می‌شود. در بخش‌های بعد توسیع جبری معرفی می‌شود. همچنین برای هر چندجمله‌ای با ضرایب در یک میدان توسیعی از آن میدان می‌یابیم که شامل حداقل یک ریشه از چندجمله‌ای مفروض باشد. این توسیع را توسیع کرونگر^۱ می‌نامیم. همچنین با انتخاب یک ریشه از یک چندجمله‌ای با ضرایب در یک میدان و الحاق این ریشه به میدان ضرایب، توسیع جدیدی با نام توسیع الحاقی به دست می‌آید. در ادامه این فصل نشان می‌دهیم که توسیع الحاقی و توسیع کرونگر یکریخت هستند. در بخش‌های انتهایی این فصل میدان شکافنده یک چندجمله‌ای با ضرایب در یک میدان دلخواه را معرفی می‌کنیم که این میدان شامل همهٔ ریشه‌های چندجمله‌ای مفروض است. سرانجام برای هر میدان دلخواه و هر چندجمله‌ای دلخواه با ضرایب در آن میدان، میدانی ساخته می‌شود که شامل همه ریشه‌های آن چندجمله‌ای باشد. این میدان را بستار جبری میدان مفروض می‌نامیم.

فصل چهارم مقدمه‌ای بر نظریهٔ گالوا است. در این فصل ابتدا توسیع نرمال و جداپذیر را مطالعه و بررسی می‌کنیم، سپس توسیع گالوای یک میدان را معرفی و خواص آن را به دقت بررسی می‌کنیم. همچنین برای هر توسیع گالوا از یک میدان، گروه گالوای آن را به دست می‌آوریم. یکی از نتایج مهم این فصل، مقایسه درجهٔ توسیع گالوا با مرتبهٔ گروه گالوای آن است. به بیان دقیق‌تر نشان می‌دهیم درجهٔ توسیع گالوا با مرتبهٔ گروه گالوای متناظرش برابر است. هدف اصلی این فصل بررسی قضیه بنیادی گالوا است. در این قضیه تناظر یک‌به‌یکی بین میدان‌های میانی و زیرگروه‌های گروه گالوا ایجاد می‌شود.

در فصل پنجم کاربرد نظریهٔ گالوا را در مسائل ترسیم‌پذیری می‌بینیم. در این فصل ترسیم‌پذیری اعداد تنها به کمک خط‌کش و پرگار تعریف می‌شود. سپس مسائل چهارگانه و قدیمی ترسیم‌پذیری؛ یعنی مضاعف کردن یک مکعب، تربیع یک دایره، تثلیث یک زاویه و ترسیم‌پذیری یک چندضلعی منتظم بررسی می‌شود. برای این منظور ابتدا نشان می‌دهیم که مجموعه اعداد ترسیم‌پذیر یک زیر میدان از اعداد حقیقی تشکیل می‌دهند. سپس با استفاده از قضایای توسیع‌ها نشان می‌دهیم که مضاعف کردن مکعب، تربیع دایره و تثلیث زاویه امکان‌پذیر نیست. همچنین نشان می‌دهیم که ترسیم برخی از چندضلعی‌های منتظم تنها به

1. L. Kronecker

کمک خط‌کش و پرگار امکان‌پذیر نیست.

در پایان کتاب پیوستی ارائه شده است که شرح مختصری از زندگی‌نامه ریاضی‌دانان بزرگ و نامی ایران و جهان است. این ریاضی‌دانان در زمینه جبر تحقیقات ارزنده‌ای انجام داده‌اند و در تکمیل و اشاعه نظریه گالوا نقش به‌سزایی داشته‌اند. این پیوست در دو بخش، ریاضی‌دانان ایرانی و ریاضی‌دانان غربی تنظیم شده است.

در پایان لازم می‌دانم که از داوران محترم این اثر علمی و همچنین از ویراستار علمی محترم، سرکار خانم دکتر خدیجه احمدی آملی تشکر و قدردانی نمایم. بی‌تردید پیشنهادات علمی و نگارشی ارزنده و دقیق ویراستار محترم، شرایط را برای تالیف کتابی خودآموز و شایسته دانشجویان ریاضی، مهیا نموده است.

سعادت‌اله فرامرزی

تابستان ۱۳۹۴

فصل ۱

گروه‌های حل‌پذیر

هدف کلی

در این فصل سری‌های نرمال، ترکیبی و حل‌پذیر را معرفی و گروه‌های حل‌پذیر را به طور دقیق بررسی می‌کنیم.

هدف‌های یادگیری

انتظار می‌رود دانشجو پس از مطالعه این فصل بتواند:

۱. مفاهیم مقدماتی و قضایای گروه را در ذهن خود تداعی کند و آن‌ها را در بخش‌های بعد به کار برد.
۲. سری نرمال و زیرنرمال و وجه تمایز آن‌ها را با ارائه مثال شرح دهد.
۳. مفهوم سری ترکیبی و اصلی را توضیح دهد.
۴. سری ترکیبی را برای گروه‌های متناهی و نامتناهی با بیان قضیه مشخص کند.
۵. قضیه شرایر را بیان و اثبات کند.
۶. قضیه ژردان-هلدر را بیان و اثبات کند.
۷. گروه حل‌پذیر را تعریف و ارتباط آن را با گروه مشتق بیان کند.
۸. نشان دهد که برای هر $m \geq 5$ گروه S_m حل‌پذیر نیست.
۹. شرط لازم و کافی برای حل‌پذیری یک گروه بر اساس عامل‌های نرمال را بیان و اثبات کند.
۱۰. ارتباط حل‌پذیری یک گروه را با حل‌پذیری زیرگروه‌ها و گروه خارج قسمتی آن بیان کند.
۱۱. ارتباط بین سری حل‌پذیر با سری ترکیبی را در یک گروه متناهی بیان کند.

۱۲. ارتباط حل‌پذیری یک گروه را با متناهی بودن سری مشتق آن بیان کند.

مقدمه

یکی از شاخه‌های قدیمی جبر، نظریه گروه‌هاست. نظریه گروه‌ها ارتباط تنگاتنگی با نظریه معادلات دارد و به جرئت می‌توانیم بگوییم که خاستگاه نظریه گروه‌ها، نظریه معادلات است. بی‌تردید یکی از زیبایی‌های نظریه معادلات، یافتن ریشه‌های یک چندجمله‌ای است. پیدا کردن قاعده کلی برای ریشه‌های یک چندجمله‌ای با درجه بزرگ‌تر از سه، تا مدت مدیدی یکی از مسائل مورد علاقه جبريست‌ها بوده است. در ابتدای قرن نوزدهم میلادی هنریک آبل^۱ نشان داد که ممکن است فرمولی کلی برای پیدا کردن ریشه‌های یک چندجمله‌ای وجود نداشته باشد. تحقیقات اساسی در ارتباط با حل‌پذیری چندجمله‌ای‌ها توسط ریاضی‌دان برجسته اواريست گالوا^۲ انجام شد. وی در سال ۱۸۳۰ برای اولین بار به این مسئله جواب داد. گالوا به هر چندجمله‌ای یک گروه جایگشتی از ریشه‌های آن مرتبط کرد. وی نشان داد: «یک چندجمله‌ای با درجه n حل‌پذیر است اگر و تنها اگر گروه جایگشتی وابسته به آن حل‌پذیر باشد.»

از این‌رو نظریه گالوا نقش به‌سزایی در پیشرفت جبر دارد، زیرا در این نظریه، حل‌پذیری یک چندجمله‌ای به حل‌پذیری گروه گالوای آن وابسته است.

۱-۱ مروری بر نظریه گروه‌ها

در این بخش به‌طور مختصر مفاهیم و قضایای نظریه گروه‌ها را که در بخش‌های بعد مورد نیاز است، یادآوری می‌کنیم. فرض بر این است که خواننده با قضایای این بخش در نظریه گروه‌ها آشنا شده است و اثبات آنها را درس مبانی جبر مشاهده کرده است.

تعریف ۱-۱-۱. مجموعه G با عمل دوتایی $*$ را یک گروه نامیم و با زوج مرتب $(G, *)$ نشان می‌دهیم هرگاه شرایط ذیل برقرار باشد.

(الف) عمل $*$ شرکت‌پذیر باشد. یعنی، به ازای هر $a, b, c \in G$ تساوی $a * (b * c) = (a * b) * c$

1. Niels Henrik Abel

2. Evariste Galois

$(a * b) * c$ برقرار باشد.

ب) مجموعه G نسبت به عمل $*$ عضو خنثی داشته باشد. یعنی، عضوی مانند $e \in G$ وجود داشته باشد که به ازای هر $a \in G$ تساوی $a * e = e * a = a$ برقرار باشد.

ج) هر عضو G نسبت به عمل $*$ وارون داشته باشد. یعنی، به ازای هر عضو $a \in G$ عضوی مانند $a' \in G$ وجود داشته باشد که $a * a' = a' * a = e$.

برای مطابقت با آنچه در اعداد صحیح و اعداد حقیقی رخ می‌دهد به جای علامت $*$ از علامت ضرب و جمع استفاده می‌کنیم. همچنین از آنجا که عضو وارون در یک گروه منحصر به فرد است، معمولاً وارون عضو a را با a^{-1} و در یک گروه جمعی با $-a$ نشان می‌دهیم. از این پس گروه G را ضربی در نظر می‌گیریم.

تعریف ۱-۱-۲. گروه G را یک **گروه آبلی** گوئیم، هرگاه عمل آن خاصیت جابجایی داشته باشد. به عبارت دیگر به ازای هر $x, y \in G$ $xy = yx$.

تعریف ۱-۱-۳. گروه G را یک **گروه دوری** گوئیم، هرگاه عضوی مانند $a \in G$ وجود داشته باشد که

$$G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}.$$

قضیه ۱-۱-۴. هر گروه دوری یک گروه آبلی است.

گروه‌های $(\mathbb{Z}, +) = \langle 1 \rangle$ و $(\mathbb{Z}_n, \oplus_n) = \langle [1] \rangle$ گروه‌هایی دوری و آبلی هستند و این در حالی است که گروه چهارتایی کلاین آبلی است ولی دوری نیست. (گروه چهارتایی کلاین که با K_4 نمایش داده می‌شود عبارت است از گروه چهار عضوی $K_4 = \{e, a, b, c\}$ که در آن $a^2 = b^2 = c^2 = e$ و همچنین $ab = c$ و $bc = a$ و $ca = b$).

تعریف ۱-۱-۵. فرض کنیم G یک گروه و $H \subseteq G$. در این صورت H را یک **زیرگروه** G نامیم هرگاه H تحت عمل G ، یک گروه باشد. در این حالت می‌نویسیم $H \leq G$. لازم به ذکر است که اگر $H \neq G$ ، آنگاه نماد $H < G$ را به کار می‌بریم.

به وضوح G و $\langle e \rangle$ دو زیرگروه G هستند. این دو زیرگروه را زیرگروه‌های بدیهی G می‌نامیم.

قضیه ۱-۱-۶. فرض کنیم G یک گروه و H یک زیرمجموعه ناتهی آن باشد. در این صورت
 $H \leq G$ اگر و تنها اگر

(الف) وارون هر عضو H متعلق به خود H باشد. یعنی، به ازای هر $a \in H$ ، $a^{-1} \in H$.

(ب) به ازای هر $a, b \in H$ ، $ab \in H$.

برای مثال، زیرگروه‌های $\mathbb{Z}$ به صورت $n\mathbb{Z}$ هستند که در آن $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$.

تعریف ۱-۱-۷. تعداد اعضای یک گروه را **مرتبه** آن گروه می‌نامیم. اگر این تعداد متناهی باشد، **گویییم گروه متناهی** است و در غیر این صورت آن را **گروه نامتناهی** می‌نامیم. مرتبه گروه G را با نماد $|G|$ نشان می‌دهیم.

تعریف ۱-۱-۸. فرض کنیم G یک گروه و $a \in G$. در این صورت کوچک‌ترین عدد طبیعی مانند n که $a^n = e$ را **مرتبه عضو** a می‌نامیم و می‌نویسیم $o(a) = n$. اگر چنین عدد طبیعی وجود نداشته باشد، گویییم مرتبه عضو نامتناهی است.

اگر $G = \langle a \rangle$ یک گروه دوری باشد، آیا مرتبه گروه با مرتبه مولدش برابر خواهد بود؟ همچنین آیا این گروه مولد دیگری غیر از a نیز دارد؟ آیا زیرگروه‌های G نیز دوری هستند؟ در صورت مثبت بودن جواب، مولدهای زیرگروه چگونه به دست می‌آیند و چه ارتباطی با مولدهای گروه دارند؟ دو قضیه زیر به این پرسش‌ها پاسخ می‌دهد و ساختار زیرگروه‌های یک گروه دوری را مشخص می‌کند.

قضیه ۱-۱-۹. فرض کنیم $G = \langle a \rangle$ یک گروه دوری از مرتبه n و $H \leq G$. در این صورت

(الف) $o(a) = n$.

(ب) H نیز دوری است و $H = \langle a^m \rangle$ که در آن m کوچک‌ترین عددی است که $a^m \in H$.

(ج) به ازای هر $t \in \mathbb{N}$ داریم $o(a^t) = \frac{n}{(n, t)}$ که در آن (n, t) بزرگ‌ترین مقسوم علیه مشترک n و t است.

(د) اگر $s \mid n$ ، آنگاه G زیرگروهی از مرتبه s دارد.

قضیه ۱-۱-۱۰. فرض کنیم $G = \langle a \rangle$ یک گروه دوری باشد. در این صورت

(الف) وارون هر مولد G نیز یک مولد G است. علاوه بر این اگر G نامتناهی باشد، آنگاه مولدهای G فقط a و a^{-1} هستند.

(ب) اگر G متناهی از مرتبه n باشد، آنگاه $G = \{e, a, a^2, \dots, a^{n-1}\}$.

(ج) اگر G متناهی از مرتبه n باشد، آنگاه بقیه مولدهای G به صورت a^m هستند که در آن $(n, m) = 1$.

تعریف ۱-۱-۱۱. فرض کنیم $X = \{1, 2, \dots, n\}$. در این صورت مجموعه توابع یک‌به‌یک و پوشا از X به X با عمل ترکیب توابع یک گروه تشکیل می‌دهند که آن را **گروه متقارن از درجه n** می‌نامیم و با علامت S_n نشان می‌دهیم. هر یک از اعضای S_n را یک جایگشت می‌نامیم. عضو همانی این گروه را با ε نمایش می‌دهیم. همچنین واضح است که مرتبه این گروه برابر $n!$ است.

تعریف ۱-۱-۱۲. فرض کنیم $A = \{1, 2, \dots, n\}$ و $i_1, i_2, \dots, i_k$ اعدادی متمایز از مجموعه A باشند. در این صورت جایگشت $\sigma \in S_n$ را یک **دور به طول k** می‌نامیم هرگاه

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1,$$

و به ازای هر $t \in A$ که $t \neq i_1, i_2, \dots, i_k$ داشته باشیم $\sigma(t) = t$. برای راحتی کار، دور σ را به صورت $(i_1 \ i_2 \ \dots \ i_k)$ نشان می‌دهیم.

به عنوان مثال دور $(1 \ 3 \ 4)$ در S_5 عبارت است از جایگشت σ که در آن

$$\sigma(1) = 3, \sigma(3) = 4, \sigma(4) = 1, \sigma(2) = 2, \sigma(5) = 5$$

مثال ۱-۱-۱۳. اعضای S_3 به صورت زیر هستند

$$S_3 = \{\varepsilon, f, f^2, g, fg, f^2g\},$$

که در آن $f = (1 \ 2 \ 3)$ و $g = (2 \ 3)$. همچنین S_3 دو زیرگروه غیر بدیهی $\langle f \rangle$ و $\langle g \rangle$ با مرتبه (به ترتیب) ۳ و ۲ دارد.

تعریف ۱-۱-۱۴. هر جایگشت به طول ۲، به صورت $(i \ j)$ را یک **ترانهش** گوئیم. بر این اساس هر جایگشت که به حاصل ضرب تعداد زوج (فرد) ترانهش تجزیه شود را یک **جایگشت زوج (فرد)** گوئیم. به وضوح جایگشت ε زوج است زیرا برای هر i, j ،

$$\varepsilon = (i \ j)(i \ j)$$

مجموعه جایگشت‌های زوج گروه S_n یک زیرگروه تشکیل می‌دهند که آن را **گروه متناوب از درجه n** می‌نامیم و با A_n نشان می‌دهیم.

برای مثال $A_3 = \{\varepsilon, (1 \ 2 \ 3), (1 \ 3 \ 2)\} = \langle f \rangle$.

قضیه ۱-۱-۱۵. به ازای هر $n \in \mathbb{N}$ داریم $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.

تعریف ۱-۱-۱۶. فرض کنیم $n \geq 3$. در این صورت مجموعه تقارن‌های یک n -ضلعی منتظم متشکل از دوران‌ها و انعکاس‌ها نسبت به محورهای تقارن با عمل ترکیب، یک گروه تشکیل می‌دهند. این گروه را **گروه دووجهی** می‌نامیم و با نماد D_n نشان می‌دهیم.

عمل ضرب گروه دووجهی D_n به گونه‌ای است که اگر f, g دو تقارن از D_n باشند، آنگاه $f.g$ به معنای آن است که ابتدا f و سپس g عمل می‌کند.

قضیه ۱-۱-۱۷. فرض کنیم $n \geq 3$. در این صورت گروه D_n نسبت به محورهای تقارن، n دوران و همچنین n انعکاس دارد. به ویژه مرتبه گروه D_n برابر $2n$ است.

قضیه زیر نشان می‌دهد که برای هر $n \geq 3$ ، گروه دووجهی D_n یک گروه دوری نیست.

قضیه ۱-۱-۱۸. گروه دووجهی D_n به صورت $\{1, a, \dots, a^{n-1}, b, ba, \dots, ba^{n-1}\}$ است که در آن $o(a) = n$ و $o(b) = 2$.

اکنون زیرگروه‌های خاصی از یک گروه را معرفی می‌کنیم که عامل اساسی در به دست آوردن گروه‌های خارج قسمتی هستند. در واقع خوش تعریفی ضرب یک گروه خارج قسمتی، مرهون خاصیت این نوع زیرگروه‌هاست.

تعریف ۱-۱-۱۹. فرض کنیم G یک گروه و $H \leq G$. در این صورت به ازای هر $a \in G$ زیر مجموعه $aH = \{ah : h \in H\}$ را یک هم‌مجموعه چپ H در G شامل a و $Ha = \{ha : h \in H\}$ را یک هم‌مجموعه راست H در G شامل a می‌گوییم. به وضوح اگر $a \in H$ ، آنگاه $aH = H = Ha$. به عبارت دیگر، در تشکیل یک هم‌مجموعه اعضای H جذب می‌شوند.

قضیه ۱-۱-۲۰. فرض کنیم G یک گروه و H زیرگروهی از آن باشد. در این صورت

(الف) اگر R و L به ترتیب مجموعه هم‌مجموعه‌های راست و چپ H در گروه G باشند، آنگاه R و L افزازهایی از G هستند. به علاوه، این دو مجموعه هم‌عددند.

(ب) به ازای هر $a \in G$ ، $|aH| = |H| = |Ha|$.

تعریف ۱-۱-۲۱. عدد اصلی $|R| = |L|$ در قضیه ۱-۱-۲۰ را اندیس H در G می‌نامیم و آن را با علامت $(G : H)$ نمایش می‌دهیم.

فرض کنیم H یک زیرگروه G باشد. رابطه $\sim$ روی G را به صورت زیر تعریف می‌کنیم.

$$x \sim y \iff x^{-1}y \in H$$

به راحتی می‌توانیم نشان دهیم که این رابطه، یک رابطه هم‌ارزی است. این هم‌ارزی و قضیه زیر، به وضوح نشان می‌دهد که مجموعه هم‌مجموعه‌های چپ یک گروه، افزازی برای آن گروه است.

قضیه ۱-۱-۲۲. فرض کنیم G یک گروه و $H \leq G$. در این صورت به ازای هر $x, y \in G$ داریم

$$xH = yH \iff x^{-1}y \in H$$

قضیه ۱-۱-۲۳. ^۱(لاگرانژ) مرتبه هر زیرگروه مرتبه گروه را عاد می‌کند.

نتیجه ۱-۱-۲۴. هر گروه از مرتبه عدد اول، یک گروه دوری است.

تعریف ۱-۱-۲۵. فرض کنیم G یک گروه باشد. زیرگروه H در G را **نرمال** گوئیم، هرگاه برای هر $h \in H$ و هر $g \in G$ ، $ghg^{-1} \in H$. نرمال بودن H در G را با نماد $H \trianglelefteq G$ نمایش می‌دهیم.

در مثال ۱-۱-۱۳ به راحتی می‌توانیم نشان دهیم که زیرگروه $\langle f \rangle$ در گروه S_3 نرمال است ولی زیرگروه $\langle g \rangle$ در S_3 نرمال نیست.

ملاحظه ۱-۱-۲۶. فرض کنیم G یک گروه و H و K زیرگروههایی از آن باشد.

(الف) اگر $H \trianglelefteq G$ و $H \leq K \leq G$ آنگاه به راحتی نتیجه می‌شود که $H \trianglelefteq K$.

(ب) نرمال بودن زیرگروه‌های یک گروه خاصیت تعدی ندارد. برای مثال زیرگروه‌های $H_1 = \{\varepsilon, (1\ 2)(3\ 4)\}$ و $H_2 = \{\varepsilon, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ از A_4 را در نظر می‌گیریم. در این صورت $A_4 \trianglelefteq H_2 \trianglelefteq H_1$ ، اما می‌توانیم نشان دهیم که زیرگروه H_1 در A_4 نرمال نیست.

قضیه ۱-۱-۲۷. فرض کنیم G یک گروه و $H \leq G$. در این صورت گزاره‌های زیر با هم معادلند.

(الف) H در G نرمال است.

(ب) هر هم‌مجموعهٔ چپ H در G یک هم‌مجموعهٔ راست در G است. یعنی برای هر $g \in G$ داریم $gH = Hg$

(ج) برای هر $g \in G$ داریم $gHg^{-1} = H$.

واضح است که همهٔ زیرگروه‌های یک گروه آبلی نرمال هستند. در قضیهٔ بعد محک مهمی برای نرمال بودن یک زیرگروه بیان می‌شود.

قضیه ۱-۱-۲۸. فرض کنیم H زیرگروهی از G باشد. در این صورت

(الف) اگر اندیس H در G برابر ۲ باشد، آنگاه H در G نرمال است.

(ب) اگر G هیچ زیرگروه دیگری از مرتبهٔ H نداشته باشد، آنگاه H در G نرمال است.

نتیجه ۱-۱-۲۹. به ازای هر $n > 1$ ، A_n در S_n نرمال است.

قضیه ۱-۱-۳۰. فرض کنیم G یک گروه و $H \leq G$. در این صورت

(الف) مجموعه $N(H) = \{g \in G : g^{-1}Hg = H\}$ یک زیرگروه G و شامل H است.

(ب) $H \trianglelefteq N(H)$. به عبارت دیگر $N(H)$ بزرگ‌ترین زیرگروه G است که H در آن نرمال است.

(ج) اگر H زیرگروه نرمال G باشد، آنگاه $G = N(H)$.

فرض کنیم G یک گروه و $H \leq G$. اگر H در G نرمال باشد، آنگاه مجموعه هم‌مجموعه‌های چپ H در G با عمل ضرب $(ab)H := aH.bH$ (به ازای هر $a, b \in G$)، یک گروه تشکیل می‌دهند. این گروه را **گروه خارج قسمتی** G به وسیله H می‌نامیم و با نماد $\frac{G}{H}$ نمایش می‌دهیم. از قضیه لاگرانژ نتیجه می‌شود که اگر G متناهی باشد، آنگاه گروه خارج قسمتی $\frac{G}{H}$ نیز متناهی است و به علاوه $|\frac{G}{H}| = \frac{|G|}{|H|}$.

تعریف ۱-۱-۳۱. فرض کنیم G یک گروه و $a, b \in G$. در این صورت $aba^{-1}b^{-1}$ را یک **جابجاگر** G می‌نامیم و آن را با علامت $[a, b]$ نمایش می‌دهیم. زیرگروه تولید شده توسط مجموعه جابجاگرهای G را **زیرگروه مشتق** G می‌گوییم و با نماد G' نشان می‌دهیم.

قضیه ۱-۱-۳۲. فرض کنیم G یک گروه باشد. در این صورت

(الف) G آبلی است اگر و تنها اگر $G' = \langle e \rangle$.

(ب) زیرگروه G' در G نرمال است.

(ج) گروه خارج قسمتی $\frac{G}{G'}$ آبلی است.

(د) به ازای هر زیرگروه نرمال H از G مانند H گروه $\frac{G}{H}$ آبلی است اگر و تنها اگر $G' \leq H$.

(ه) برای هر زیرگروه H از G داریم $H' \leq G'$.