基本

代数

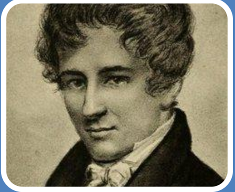
网络空间安全学院 胡丽琴

● 代数方程的解

引言

- 2000多年前，古希腊数学家就能够利用开方法解二次方程$ax^2+bx+c=0$。十六世纪初欧洲文艺复兴时期之后，求解高次方程成为欧洲代数学研究的一个中心问题。
- 1545年，意大利数学家卡尔达诺给出了三、四次多项式的求根公式
- 在此后的将近三个世纪中，人们力图发现五次方程的一般求解方法，但都失败了。

代数方程的解



直到1824年，一位年青的挪威数学家Abel才证明五次和五次以上的一般代数方程没有求根公式。

但是，人们仍然不知道什么条件之下一个已知的多项式可以通过加、减、乘、除有理运算及开方的方法求出它的所有根，什么条件之下不能求根。

最后解决这一问题的是法国年青数学家伽罗瓦。伽罗瓦引进扩域以及群的概念，并采用了一种全新的理论方法发现了高次代数方程可解的法则。

伽罗瓦理论

- 被誉为天才数学家的伽罗瓦是近世代数的创始人之一，他深入研究了一个方程能用根式求解所必须满足的本质条件，他提出的“伽罗瓦域”、“伽罗瓦群”和“伽罗瓦理论”都是近世代数所研究的最重要课题。伽罗瓦群理论被公认为十九世纪最杰出的数学成就之一。
- 伽罗瓦群还给出了几何图形能否用尺规作图的一般判别法，圆满解决了三等分任意角或倍立方题的为题都是不可解的。

基本代数

主要内容

一 群

二 域

1 群

● 二元运算

定义

定义6.1.1 设S是一个非空集合，那么S×S到S的映射叫做S的结合法或**二元运算**；对于这个映射，元素(a,b)的像叫做a与b的**乘积**，记成$a\otimes b$或$a\cdot b$或$a*b$等，为方便起见，该乘积的商简记为ab，这个结合法叫做乘法。

二元运算

- **结合律**：如果对于S中的任意元素a, b, c，都有$(ab)c=a(bc)$

交换律：如果对于S中的任意元素a, b,，都有$ab=ba$

单位元e：设S是一个具有二元运算的非空集合。如果S中存在一个元素e，使得$ae=ea=a$，对S中所有元素a都成立

●二元运算

- 如果S中的二元运算满足交换律，这个二元运算经常也被称为加法，元素(a,b)的像叫做a与b的和，记成$a\oplus b$或$a+b$。

- 当S的二元运算记成加法时，满足$a+e=e+a=a$的e叫做S中的零元，通常记做0。

● 二元运算

逆元

- **性质6.1.1** 设S是一个具有二元运算的非空集合。若S中有单位元e，则e是唯一的。

- 可逆元：设S是一个具有二元运算的有单位元e的非空集合。a是S中的一个元素。如果S中存在一个元素a'使得

$$aa'=a'a=e$$

则称a为S中的可逆元，称a'为a的逆元，通常记做a^{-1}。

二元运算

- 当S的二元运算记成加法时，满足 $aa'=a'a=e$ 的 a' 叫做 a 的**负元**，通常记做 $-a$。
- **性质6.1.2** 设S是一个具有二元运算和单位元的非空集合，则对S中任意可逆元 a，其逆元 a' 是唯一的。

● 群的定义

- **定义6.1.2** 设G是一个具有二元运算的非空集合，如果
  - G上的二元运算满足结合律
  - G中存在单位元
  - G中的每个元素都有逆元

那么G叫做一个群。

● 特殊群

- 设G是群，如果集合G是有限集合，则称G是**有限群**，G中的元素个数称为该有限群的**阶数**，记为|G|。阶数为1的群称为**平凡群**。如果G是无限集，则称G为**无限群**。

- 设G是群，若群G中的二元运算还满足交换律，则称G是**交换群**或**Abel群**。

群的例子

例

- 自然数集$\mathbf{N}=\{0, 1, 2,\ldots, n, \ldots\}$对于通常意义下的加法是否构成群？对于通常意义下的乘法是否构成群？
- 整数集$\mathbf{Z}=\{\ldots, -n,\ldots, -2, -1, 0, 1, 2,\ldots, n,\ldots\}$对于通常意义下的加法和乘法是否构成群？有理数集$\mathbf{Q}$、实数集$\mathbf{R}$和复数集$\mathbf{C}$呢？

群的例子

- 设n是正整数，令集合$\mathbf{Z}/n\mathbf{Z}=\{0,1,\ldots,n-1\}$，则集合$\mathbf{Z}/n\mathbf{Z}$对于加法

$$i \oplus j = (i + j \pmod n)$$

构成一个交换加群，其中$i \pmod n$表示整数i模n的最小非负剩余。

- 零元是什么？元素的逆元(负元)是什么？

● 群的例子

- 设p是一个素数，令集合$\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$，设$\mathbf{F}_p^*=\mathbf{F}_p\backslash\{0\}$，则集合$\mathbf{F}_p^*$对于乘法

$$i \otimes j = (i \times j \pmod n)$$

构成一个交换乘群。

- $\mathbf{F}_p^*$的单位元是1，i的逆元是$i^{-1} \pmod n$。
- 设n是一个合数，则集合$(\mathbf{Z}/n\mathbf{Z})\backslash\{0\}$对于乘法

$$i \otimes j = (i \times j \pmod n)$$

不构成一个乘群。为什么？

群的例子

- 设n是一个合数，令$(\mathbf{Z}/n\mathbf{Z})^*=\{i\ |\ i\in\mathbf{Z}/n\mathbf{Z}, (i, n)=1\}$，则集合$(\mathbf{Z}/n\mathbf{Z})^*$对于乘法

$$i\otimes j=(i\times j\ (\mathrm{mod}\ n))$$

构成一个交换乘群。

- $(\mathbf{Z}/n\mathbf{Z})^*$的单位元是1，$i$的逆元是$i^{-1}(\mathrm{mod}\ n)$。

多个元素的运算

- 设$a_1, a_2, \ldots, a_{n-1}, a_n$是群G中的$n$个元素。通常归纳地定义这$n$个元素的乘积为

$$a_1a_2\ldots a_{n-1}a_n=(a_1a_2\ldots a_{n-1})a_n.$$

- 当G的运算叫做加法时，通常归纳地定义这n个元素的和为$a_1+a_2+\ldots+a_{n-1}+a_n=(a_1+a_2+\ldots+a_{n-1})+a_n$.

● 子群

- **性质6.1.5** 设a是群G中的任意元素，则对任意的整数m, n，我们有

$$a^m a^n = a^{m+n},\ (a^m)^n = a^{mn}.$$

- **定义6.1.3** 设H是群G的一个子集。如果对于群G的二元运算，H称为一个群，那么H就叫做G的子群，记作H≤G。

子群

- H={e}和H=G都是群G的子群，叫做群G的**平凡子群**。群G的子群H叫做群G的**真子群**，如果H是群G的真子集。

- 子群的例子

➢ 设n是一个正整数，则$n\mathbf{Z}=\{nk \mid k\in\mathbf{Z}\}$是**Z**的子群。

➢ 整数集**Z**是有理数集**Q**的加法子群，非零有理数集$\mathbf{Q}^*$是非零实数集$\mathbf{R}^*$的子群。

子群判定

- **定理6.1.1** 设H是群G的一个非空子集，则H是群G的子群的充要条件是：对任意的a, b∈H，都有ab^{-1}∈H。

- 设G是一个群，X是G的非空子集，是否存在包含X的G的子群？唯一吗？

● 循环群

定义

- X的元素称为子群<X>的生成元。如果X={$a_1, \ldots, a_n$}，则记<X>为<$a_1, \ldots, a_n$>。如果G=<$a_1, \ldots, a_n$>，则称G是有限生成的。
- 特别地，如果G=<a>，则称G为由a生成的**循环群**。

● 循环群例子

- 对任意的$a\in G$，有$\langle a\rangle=\{a^n \mid n\in \mathbf{Z}\}$.
- **例** 设p=13，则模p存在原根2，从而有 $\mathbf{Z}_{13}^{*}=<2>$。
  - 可以验证$<8>$是$\mathbf{Z}_p^{*}$的一个子群。
  - **例** 设$G=\langle g\rangle=\{g^r \mid g^r \neq 1, 1\leq r< n, g^n=1\}$，G是$n$阶循环群，则$\langle g^d\rangle=\{g^{dk} \mid k\in \mathbf{Z}\}$是G的子群。
- **例** 给出加法群$\mathbf{Z}/6\mathbf{Z}$的所有子群。

● 陪集

- 设H是群G的子群，a是G中任意元素，
  - 集合$aH = \{\, ah \mid h \in H \,\}$称为G中H的**左陪集**
  - 集合$Ha = \{\, ha \mid h \in H \,\}$称为G中H的**右陪集**

aH中的元素叫做aH的代表元，Ha中的元素叫做Ha的代表元。如果aH=Ha，aH叫做G中H的陪集。

● 陪集的例子

例

■ **例** 设$n>1$是整数，则$H=n\mathbf{Z}$是$\mathbf{Z}$的子群，子集

$$a+n\mathbf{Z}=\{a+nk \mid k\in\mathbf{Z}\}$$

就是$n\mathbf{Z}$的陪集。这个陪集就是模n的剩余类。

陪集性质

- **定理6.1.5** 设H是群G的子群，则
  - 对于任意的$a\in G$，有$aH=\{c \mid c\in G,\ c^{-1}a\in H\}$；
  - 对于任意的$a, b\in G$，$aH=bH$当且仅当$b^{-1}a\in H$；
  - 对于任意的$a, b\in G$，$aH\cap bH=\varnothing$的充要条件是$b^{-1}a\notin H$；
  - 对于任意的$a\in H$，有$aH=H=Ha$。

● Lagrange定理

- 设H是群G的子群，则H在G中不同左陪集组成的新集合$\{\, aH \mid a \in G \,\}$，叫做H在G中的商集，记作G/H。G/H中不同的左陪集个数称为H在G中的指数，记作[G: H]。

- **Lagrange定理**：设H是群G的子群，则

$$|G| = [G: H] \times |H|。$$

更进一步，如果K, H是群G的子群，且K是H的子群，则

$$|G| = [G: H] \times [H: K] \times |K|。$$

● 循环群性质

定理

- **定理6.1.11** 整数加群Z的每个子群H都是循环群，并且有$H=<0>$或$H=<m>=m\mathbf{Z}$，其中m是H中的最小正整数。如果$H\neq<0>$，则H是无限的。

- **定理6.1.12** 每个无限循环群都同构于整数加群Z。每个阶为m的有限循环群同构于加群$\mathbf{Z}/m\mathbf{Z}$。

循环群性质

- **定义6.1.10** 设G是一个群，$a \in G$，则子群$\langle a\rangle$的阶称为元素a的阶，记为$\mathrm{ord}(a)$。
- 设$p=13$，2是模13的原根，从而有$\mathbf{Z}_{13}^{*}=\langle 2\rangle$。$8 \in \mathbf{Z}_{13}^{*}$，$\mathrm{ord}(8)$与$\mathrm{ord}_{13}(8)$有什么关系？

● 循环群性质

- **定理6.1.13** 设G是一个群，$a \in G$。如果a是无限阶元素，
  - $a^k=e$当且仅当$k=0$，其中e是G的单位元；
  - 元素$a^k\,(k\in \mathbf{Z})$两两不同。

如果a具有有限阶$m>0$，则

- m是使得$a^m=e$的最小正整数；
- $a^k = e$的充要条件是$m \mid k$；
- 元素$a^k\,(k\in \mathbf{Z}/m\mathbf{Z})$两两不同；
- $<a>=\{a, a^2,\ldots,a^{m-1},a^m=e\}$；
- 对于任意的整数d，$1\le d\le m$，有$\mathrm{ord}(a^d)= n/\gcd(d,n)$。

● 循环群性质

性质

- **定理6.1.14** 循环群的子群是循环群。
- **定理6.1.5** 设G是循环群。如果G是无限的，则G的生成元为a和a^{-1}。如果G具有有限阶m，则是G的生成元是a^k当且仅当$(a, k)=1$。
- 证明：素数阶的群都是循环群。

2 域

环的定义

- 设R是具有两种运算(通常表示为加法和乘法)的非空集合。如果下列条件成立：
  - R对于加法构成一个交换群；
  - R关于乘法满足结合律；
  - R的乘法关于加法满足分配律；

那么R叫做一个环。

● 环的定义

定义

- 如果环R关于乘法满足交换律，则R叫做**交换环**。
- 如果环R中存在一个元素$e=1_R$，使得对任意的$a\in R$，有$ea=ae=a$，则R叫做**有单位元的环**。

- **定义6.2.2** 设a是环R中的一个非零元。如果存在非零元$b, c\in R$，使得$ab=0$, $ca=0$。a称为**零因子**。

● 整环

- **定义6.2.3** 设R是一个交换环。我们称R是**整环**，如果R中有单位元，但没有零因子。

 整环是满足以下条件的环：

- 交换环
- 有单位元
- 无零因子

● 环的例子

- **例** 全体整数集合**Z**对于普通的加法和乘法构成环。
- **例** 定义**Z**/m**Z**={0,1,…,m−1}上的加法和乘法分别为：

$$i+j=(i+j \bmod m)$$

$$i\times j=(i\times j \bmod m)$$

验证**Z**/m**Z**构成环，称为模m的剩余类环。

● 域

定义

- **定义6.2.4** 设a是有单位元1_R的环R中的一个元素。a称为左逆元(对应地右逆元)，如果存在$b \in R$(对应地$c \in R$)使得$ab=1_R$(对应地$ca=1_R$)。a称为逆元，如果它同时为左逆元和右逆元。
- **定义6.2.5** 设R是一个交换环。如果环R中有单位元，且每个非零元都是可逆元，则称R为域。

● 域

例子

一般用F表示域。域F满足：

- F对于加法构成一个交换群；
- $F^{*}=F\backslash\{0\}$对于乘法构成一个交换群。

- 整环不一定是域，但域一定是整环，即域没有零因子。
- **例** 全体有理数集**Q**、全体实数集**R**关于通常的加法和乘法构成域。

● 域

- **例** 设p为素数，则$\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}=\{0,1,\ldots,p-1\}$为域。
- **定义6.2.9** 设R是一个环。如果存在一个最小正整数n使得对任意$a\in$R，都有$na=0$，则称环R的**特征为n**；如果不存在这样的正整数，则称环R的**特征为零**。
- **例** 有理数域**Q**、实数域**R**的特征分别是什么？
- **例** 设m为正整数，则$\mathbf{Z}/m\mathbf{Z}=\{0, 1,\ldots, m-1\}$的特征是什么？

● 特征性质

- **定理6.2.3** 如果域K的特征不为零，则其特征必为素数。
- **定理6.2.4** 设R是有单位元的交换环。如果环R的特征是素数p，则对任意的$a,b\in R$，有

$$(a+b)^p=a^p+b^p.$$

● 多项式环

■ 例 整环R上的多项式环R[x]。设

$f(x)=a_nx^n+\ldots+a_1x+a_0\in \mathrm{R}[x]$,

$g(x)=b_nx^n+\ldots+b_1x+b_0\in \mathrm{R}[x]$,

在R[x]上定义加法

$$(f+g)(x)=(a_n+b_n)x^n+\ldots+(a_1+b_1)x+(a_0+b_0)$$

R[x]对于该加法构成一个交换加群。零元为0,

$f(x)$的负元是$(-f)(x)=(-a_n)x^n+\ldots+(-a_1)x+(-a_0)$

多项式环

例

- 设$f(x)=a_n x^n+\ldots+a_1 x+a_0 \in R[x]$，

  $g(x)=b_m x^m+\ldots+b_1 x+b_0 \in R[x]$，$a_n b_m \neq 0$在$R[x]$上定义乘法

$$(f\cdot g)(x)=c_{m+n}x^{m+n}+\ldots+c_1 x+c_0$$

其中$c_k=\sum_{i+j=k} a_i b_j$，$0\leq k\leq m+n$。

$R[x]$对该乘法运算满足结合律和交换律，有单位元1，并且有分配律。因此，$R[x]$是有单位元的交换环。

多项式环

- **例** 设$f(x)=x^6+x^4+x^2+x+1$，$g(x)=x^7+x+1\in\mathbf{F}_2[x]$，求$f(x)+g(x)$和$f(x)\times g(x)$。
- 解：$f(x)+g(x)=x^7+x^6+x^4+x^2$

  $f(x)\times g(x)=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1$

- **定义6.2.17** 设$f(x)$是整环R上的非常数的多项式。如果除了显然的因式1和$f(x)$外，$f(x)$没有其他因式，那么$f(x)$叫做**不可约多项式**；否则，$f(x)$叫做**可约多项式**或合式。

● 不可约多项式

性质

- 事实上，多项式是否可约与其所在的环或域有关。
- **例** 多项式x^2+1在整系数多项式环$\mathbf{Z}[x]$中不可约，在复系数多项式环$\mathbf{C}[x]$中是可约的，在$\mathbf{F}_2[x]$中是不是可约的？
- **例** 给出$\mathbf{F}_2[x]$中所有不可约二次多项式。

● 域

- **定义6.3.1** 给定R[x]中一个首一多项式$m(x)$。两个多项式$f(x)$, $g(x)$叫做**模$m(x)$同余**，如果$m(x)|f(x)-g(x)$，记作$f(x)\equiv g(x)(\mathrm{mod}\ m(x))$；否则叫做模$m(x)$不同余。

- **定理6.3.1** 设**K**是一个域。$p(x)$是**K**[x]中的不可约多项式，则商环**K**[x]/($p(x)$)对于多项式模加和模乘运算构成域。