1 准备知识

1.1 数域

定义1.1. 设K是复数集的一个子集,如果K满足:

(1)$0,1\in K$;

(2)对于任意的$a,b\in K$,都有$a\pm b,ab\in K$;并且当$b\neq 0$时,有$\frac{a}{b}\in K$,
那么称K是一个**数域**.

其中第(2)个条件可以说成：K对于加、减、乘、除4种运算封闭。

在平时应用中，有很多数域，如复数域C，实数域R，有理数域Q。除了C，R，Q之外，还有其他数域，例如：

$$Q(\sqrt{2})=\{a+b\sqrt{2}|a,b\in Q\}$$

容易验证，$Q(\sqrt{2})$也是一个域。

数域是一个复数的子集，在数域上进行方程组求解、矩阵的相似对角化等过程，是基于数域对加减乘除运算封闭的性质，如果集合里的元素不是复数，只要满足一定的运算性质，同样可以进行相应的运算过程，只是运算对象不再是复数，而是集合里符合运算性质的元素。下面我们介绍比数域更一般的概念。

1.2 域

定义1.2. 设F是在其上定义了两个运算（加法"$+$"、乘法"$\cdot$"）的集合，并且这两个运算满足：

(1)$(F;+)$是交换群；

(2)$(F^*;\cdot)$是交换群，其中$F^*=F\setminus\{0\}$；

(3)运算"$\cdot$"对"$+$"满足分配律，
则称F为**域**。

定义1.3. 设F是域，如果存在正整数n，使得对于每个$x\in F$都有$nx=0$，则称满足此条件的最小正整数n为域F的**特征数**。如果不存在这样的正整数n，则称域F的特征数为0。用$CharF$表示域F的特征数。

域F的特征数是素数或者0。对于有理数域Q和有限剩余类域Z_p，有$CharQ=0$，$CharZ_p=p$，其中p是素数。特征数是0的域都包含有理数域Q 作为它的一个子域。在此我们只考虑特征数为0的情况。

例：$K=\{0,1\}$在下面定义的运算下是一个域。

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

定义1.4. 设V是一个非空集合，F是一个域。在V上定义了一个代数运算：$(\alpha,\beta)\mapsto\gamma$，叫做加法，把$\gamma$称为$\alpha$和$\beta$的和，记作$\gamma=\alpha+\beta$。在$F$与$V$之间定义了一个运算，即$F\times V$到$V$的一个映射：$(k,\alpha)\mapsto\delta$，叫做纯量乘法（当$F$为数域时，也叫数量乘法），把$\delta$称为$k$与$\alpha$的纯量乘积（当$F$为数域时，也叫数量乘积），记作$\delta=k\alpha$。如果加法和数量乘法满足下述8 条运算法则：对任意的$\alpha,\beta,\gamma\in V$，任意的$k,l\in F$，有

(1) $\alpha+\beta=\beta+\alpha$ （加法交换律）；

(2) $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$ （加法结合律）；

(3) V中有一个元素，记作0，它使得

$$\alpha+0=\alpha，\forall\alpha\in V，$$

(4) 对于$\alpha\in V$，存在$\beta\in V$，使得

$$\alpha+\beta=0，$$

具有这个性质的元素β称为α的负元素；

(5) $1\alpha=\alpha$，

(6) $(kl)\alpha=k(l\alpha)$，

(7) $(k+l)\alpha=k\alpha+l\alpha$，

(8) $k(\alpha+\beta)=k\alpha+k\beta$，

则称V是域F上的一个**线性空间**。

数域K上所有n元有序数组组成的集合K^n，对于有序数组的加法与数量乘法，成为数域K上的一个线性空间。

数域K上所有$s\times n$矩阵组成的集合，对于矩阵的加法与数量乘法，成为数域K上的一个线性空间。

复数域C可以看成实数域R上的一个线性空间，而实数域R可以看成有理数域Q上的线性空间。

思考题

$2n+1$个实数有如下性质：

$(*)$任意去掉一个，余下的$2n$个可以分为2 组，每组n个，且和相等。则$2n+1$个实数必相同。

解： 设$2n+1$个实数为x_1，x_2，$\cdots$，x_{2n+1}，令$V=<x_1,x_2,\cdots,x_{2n+1}>$是$Q$上关于$R$的有限维线性子空间，不妨设$\beta_1,\cdots,\beta_s$为$V$的一组基。

则$x_i=\sum\limits_{j=1}^{s}a_{ij}\beta_j$，$(a_{ij}\in Q)$，$i=1,2,\cdots,2n+1$

假设去掉的是x_{2n+1}，剩下的$2n$个数有

$$x_1+x_2+\cdots+x_n=x_{n+1}+x_{n+2}+\cdots+x_{2n}$$
$$\sum_{i=1}^{n}x_i=\sum_{i=n+1}^{2n}x_i$$

将$x_i=\sum\limits_{j=1}^{s}a_{ij}\beta_j$ 代入上式，得

$$\sum_{i=1}^{n}\sum_{j=1}^{s}a_{ij}\beta_j=\sum_{i=n+1}^{2n}\sum_{j=1}^{s}a_{ij}\beta_j$$
$$\sum_{j=1}^{s}\sum_{i=1}^{n}a_{ij}\beta_j=\sum_{j=1}^{s}\sum_{i=n+1}^{2n}a_{ij}\beta_j$$

取定j，两边对应系数相等，有

$$\sum_{i=1}^{n}a_{ij}=\sum_{i=n+1}^{2n}a_{ij},j=1,2,\cdots,s$$

则对于固定的j，$a_{1,j},a_{2,j},\cdots,a_{2n+1,j}$也有性质$(*)$，而$a_{ij}\in Q$，则$a_{1,j}=a_{2,j}=\cdots=a_{2n+1,j}$。所以$x_1=x_2=\cdots=x_{2n+1}$。

注1.5. 题目中的域的特征数为0，假如在有限特征的域上满足性质$(*)$，结论不一定成立。例如在Z_3上，$\{1,1,2,2,0\}$就满足性质$(*)$，但它们不相等也不全是零。

1.3 环

定义1.6. 设集合R上定义了两种运算"$+$" 和"$\cdot$"，并且满足：

(1) $\{R;+\}$是交换群，

(2) "$\cdot$"满足结合律，

(3) "$\cdot$"对"$+$"满足分配律，

则称$\{R;+,\cdot\}$为**环**。

如果对于”·”有单位元，称R为幺环。

如果运算”·”满足交换律，即$a \cdot b = b \cdot a$，$\forall a, b \in R$，则称R为交换环。

例：整数环有单位元1，偶数构成的环没有单位元。

例：数域F上的一元多项式环是交换环，剩余类环Z_n是交换环。数域F上n阶方阵$M_n(F)$关于矩阵的加法和乘法运算构成非交换环。

定义1.7. 设R是一个环，如果对于R中的非零元素a，b，有$ab = 0$，则称a是环R中的**左零因子**，b是环R中的**右零因子**。

若R中的一个元素既是左零因子，又是右零因子，则称它是R中的零因子。

例：$M_n(F)$和Z_n（n不是素数）都是有零因子的环。

定义1.8. 我们称非零的，有1的，交换的，无零因子的环为**整环**。

例：整数环、实数域R上的一元多项式环$R[x]$等都是整环。

定义1.9. （欧几里得整环）设D为整环，若存在一个映射φ：$D^* \to N$，对于$\forall a, b \in D(b \neq 0)$，存在$q, r \in D$，使得$a = bq + r$，且$r = 0$或$\varphi(b) > \varphi(r)$，称$D$为**欧几里得整环**。

注1.10. 欧几里得整环是一种可以做辗转相除法的整环，函数φ可以看做是元素大小的量度。

例：整数环Z和数域K上的一元多项式环$K[x]$都为欧几里得整环。在$K[x]$中，$\varphi(f) = degf$。若$D = Z$，$\varphi(x) =\mid x \mid$。

1.4 同态

定义1.11. **同态**是两个代数结构之间保持运算关系的映射。

定义1.12. 设R和R'是环，如果存在映射$\varphi : R \longrightarrow R'$，使得映射$\varphi$保持环的运算，即对于$\forall a, b \in R$有

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = \varphi(a)\varphi(b)$$

则称φ是R到R'的环同态，也称环R与R'同态。

相应的还有群同态、域同态。对于两个线性空间来说，同态保持加法和数乘运算，线性空间的同态就是线性空间之间的线性映射。

注1.13. 若φ是$K_1 \longrightarrow K_2$的域同态，则φ一定是单射。事实上，如果对于$a \in K_1$，且$a \neq 0$，有$\varphi(a) = 0$，$\varphi(1) = \varphi(aa^{-1}) = 0$，与$\varphi(1) = 1$矛盾。

1.5 域上的多项式环

1.5.1 最大公因式

定义1.14. 对于$f(x), g(x) \in K[x]$，可以找到一个次数最大的多项式$d(x)$，使得$d(x) \mid f(x)$且$d(x) \mid g(x)$，称$d(x)$为$f(x)$和$g(x)$ 的**最大公因式**。首1的最大公因式记为$(f(x), g(x))$。

$\forall f(x), g(x) \in K[x]$，可以用欧几里得算法得到$(f(x), g(x))$，而且找到$u(x), v(x) \in K[x]$，使$(f(x), g(x)) = f(x)u(x) + g(x)v(x)$。若$f(x)$与$g(x)$互素，则$f(x)u(x) + g(x)v(x) = 1$。

1.5.2 不可约多项式

定义1.15. 在$K[x]$中，如果$f(x) \mid g(x)$且$g(x) \mid f(x)$，则称$f(x)$与$g(x)$**相伴**。

定义1.16. $K[x]$中一个次数不大于零的多项式$p(x)$，如果它在$K[x]$中的因式只有零次多项式和$p(x)$的相伴元，则称$p(x)$是数域K上的一个**不可约多项式**；否则称$p(x)$为可约多项式。

$C[x]$中不可约多项式都是一次的，$R[x]$中不可约多项式为一次的和判别式小于零的二次多项式，$Q[x]$中不可约多项式可以是任意次的，如$x^n - 2$。

定理1.17. （唯一因式分解定理）$K[x]$中每一个次数大于零的多项式$f(x)$都能唯一的分解成数域K上有限多个不可约多项式的乘积。所谓唯一性是指，如果$f(x)$有两个这样的分解式：

$$f(x) = p_1(x)p_2(x)\cdots p_s(x) = q_1(x)q_2(x)\cdots q_t(x),$$

则一定有$s = t$，且适当排列因式的次序后有

$$p_i(x) \sim q_i(x), i = 1, 2, \cdots, s.$$

在考虑因式分解问题时，整系数多项式的分解问题等价于将其视为有理系数域上的多项式分解问题。判断整系数多项式是否可约，最常用的是$Eisenstein$判别法。

定理1.18. （$Eisenstein$）设$f(x) = a_n x^n + \cdots + a_1 x^1 + a_0 \in Z[x]$。如果存在一个素数$p$，使得

(1) $p \nmid a_n$；

(2) $p \mid a_i, i = 0, 1, \cdots, n-1$；

(3) $p^2 \nmid a_0$;

则$f(x)$在有理数域上是不可约的。

在$K[x]$中，3次及3次以下的多项式可约与对应的多项式方程在数域K上有根是等价的。

下面的结论也对判断一个多项式是否可约有帮助。

定理1.19. 设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0$$

是一个整系数多项式，而$\frac{r}{s}$是它的一个有理根，其中r，s互素，那么必有$s \mid a_n$，$r \mid a_0$。

例：证明

$$f(x) = x^3 - 5x + 1$$

在有理数域上不可约。

如果$f(x)$可约，那么它至少有一个一次因式，也就是有一个有理根。但是$f(x)$的有理根只可能是± 1，代入验算可知± 1全不是根，因而$f(x)$在有理数域上不可约。

2 域的扩张

我们解方程的时候总是将它做因式分解，如果有一次因式的话，就会有相应的根，但是当方程在域上不可约的时候就没有办法解出方程的根，在代数上就会想到把域扩大，扩大之后的域可能就会有方程的根。

2.1 扩域

定义2.1. 如果集合K是域F的一个非空子集，并且K在域F的运算下构成一个域，则称K是域F的子域，或称F是K的扩域，也称F是K的扩张。

扩域F可看成子域K上的线性空间，用$[F:K]$表示F在K上的维数$dim_K F$。

例如前面提到的复数域C和实数域R，复数域C就可以看做实数域R的扩域，C作为R上的线性空间，维数为2。

定义2.2. 域K的两个扩域E，Ω，ρ是$E \longrightarrow \Omega$ 的域同态，且$\rho|_k = id$，则称ρ是$E \longrightarrow \Omega$的$K-$**同态**（$K-$**嵌入**）。

注2.3. 1.E，Ω可以看成K上的线性空间，ρ可以看成E到Ω的线性映射。

2.同构的域视为一个，不加以区分。

定理2.4. （维数公式）设$K \subseteq M \subseteq E$都是域。则$[E:K]$ 有限当且仅当$[E:M]$和$[M:K]$有限，且$[E:K]$=$[E:M][M:K]$。

证：假设$[E:M]=m$，$[M:K]=n$，E看成M上的线性空间，一组基为$\alpha_1,\cdots,\alpha_m$。M看成K上的线性空间，一组基为$\beta_1,\cdots,\beta_n$，则$\forall s \in E$，有$s=\sum\limits_{i=1}^{m} t_i\alpha_i$，$t_i \in M$。而把$M$看成$K$ 上的线性空间，有$t_i=\sum\limits_{j=1}^{n} l_{ij}\beta_j$，$l_{ij}\in K$。所以$s=\sum\limits_{i=1}^{m}\sum\limits_{j=1}^{n} l_{ij}\alpha_i\beta_j$。而$(\alpha_i\beta_j)_{1\le i\le m,1\le j\le n}$是线性无关的。故$(\alpha_i\beta_j)_{1\le i\le m,1\le j\le n}$可以作为$E$看成$K$上的线性空间的一组基，则$[E:K]=mn$。

2.2 等价类，商域

$f(x)\in K[x]$，$degf\geq 2$，$\forall h(x)\in K[x]$，有$h(x)=q(x)f(x)+r(x)$，把$K[x]$关于$f(x)$的余数分类。

$$(f(x))=\{q(x)f(x)\mid q(x)\in K[x]\}$$
$$a(x)+(f(x))=\{a(x)+q(x)f(x)\mid a(x),q(x)\in K[x]\}$$

$\forall b(x)\in(a(x)+(f(x)))$当且仅当$b(x)-a(x)=t(x)f(x),t(x)\in K[x]$。

在剩余类上可以定义"$+$","$\cdot$"：

$$(r_1(x)+(f(x)))+(r_2(x)+(f(x)))\triangleq(r_1(x)+r_2(x))+(f(x))$$
$$(r_1(x)\cdot(f(x)))+(r_2(x)+(f(x)))\triangleq r_1(x)r_2(x)+(f(x))$$

下面验证定义的合理性：

若

$$r_1'(x)+(f(x))=r_1(x)+(f(x))$$
$$r_2'(x)+(f(x))=r_2(x)+(f(x))$$

即

$$r_1'(x)-r_1(x)=t_1(x)f(x),r_2'(x)-r_2(x)=t_2(x)f(x)$$

则

$$\begin{aligned}&(r_1'(x)+r_2'(x))-(r_1(x)+r_2(x))\\=&(r_1'(x)-r_1(x))+(r_2'(x)-r_2(x))\\=&(t_1(x)+t_2(x))f(x)\end{aligned}$$

即

$$(r_1'(x)+r_2'(x))+(f(x))=(r_1(x)+r_2(x))+(f(x))$$

对于"$\cdot$", 同样可利用同余性质验证其合理性。

容易验证，$K[x]/(f(x))=$(所有剩余类;"$+$","$\cdot$")是一个环。

若$f(x)$是不可约的，$K[x]/(f(x))$是域。

只需证明，$K[x]/(f(x))$中任意元素都有逆元素。设$degf=m$，则

$$K[x]/(f(x))=\{a_0+a_1x+\cdots+a_{m-1}x^{m-1}+(f(x))\mid a_i\in K\}$$

$\forall g(x)+(f(x))\in K[x]/(f(x))$，在$K[x]$中，由欧几里得算法，存在$a(x),b(x)\in K[x]$，使得

$$a(x)f(x)+b(x)g(x)=d(x)$$

$d(x)$为$f(x)$与$g(x)$的最大公因式。

因为$f(x)$不可约且$degg < degf$，所以$d(x) = 1$，即

$$a(x)f(x) + b(x)g(x) = 1$$

而在$K[x]/(f(x))$中，$a(x)f(x) = 0 + (f(x))$，则

$$b(x)g(x) + (f(x)) = 1 + (f(x))$$

即$g(x)+(f(x))$的逆元素为$b(x)+(f(x))$（若$degb \geq m$，利用$f(x)$将$b(x)$化为次数小于m 的多项式。）

2.3 干域

为了区分多项式与方程，有些地方会用X表示多项式的未定元，用x表示方程中的元素。

由前面可知，当$f(X)$不可约时，$K[X]/(f(X))$是一个域。我们称$E = K[X]/(f(X))$为K关于$f(X)$的**干域**。可以看成K的扩域，若E看成是K上的线性空间，则$dim_K E = degf$。存在一个的同态映射$\rho : K \longrightarrow E$，使$\rho(a) = a + (f(X))$。还有在$E$ 中，$X + (f(X))$ 是$f(x) = 0$ 的一个根。

例：令$K = Q$，$f(X) = X^5 - 2X + 2 \in Q[X]$。则$Q[X]/(f(X)) = \{a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + (f(X)) \mid a_i \in Q, i = 0, 1, 2, 3, 4\}$是一个域。它的一个子域$\{q + (f(X)) \mid q \in Q\}$与$Q$同构。$Q[X]/(f(X))$可以看成$Q$上的线性空间，维数为5。$1 + (f(X))$，$X + (f(X))$，$X^2 + (f(X))$，$X^3 + (f(X))$，$X^4 + (f(X))$是一组基。

定理2.5. K的一个扩域Ω上有一个$f(X)$的根x_0，则存在一个域同态$\rho : E \longrightarrow \Omega$使$\rho(g(X) + (f(X))) = g(X_0)$。

例：设$f(X) = X^2 - 2 \in Q[X]$。Q关于$f(X)$的干域为$E = Q[X]/(f(X)) = \{aX + b + (f(X)) \mid a, b \in Q\}$。$f(X)$在$E$上有根$X + (f(X))$。而$f(X)$在$R$ 上有两个根$\sqrt{2}$和$-\sqrt{2}$，则存在同态$\rho : E \longrightarrow R$和$\rho' : E \longrightarrow R$，使$\rho(aX+b+(f(X))) = a\sqrt{2}+b$，$\rho'(aX+b+(f(X))) = a(-\sqrt{2}) + b$。$f(X)$在$R$ 上有几个根就有几个这样的同态。

注2.6. 上述例题中$Q(\sqrt{2})$与$Q(-\sqrt{2})$是同构的。由此可见，用代数的方法解方程是简单的，将域的范围不断扩大，总会有根存在，但是根的具体情况就不太容易确定了。

2.4 代数元，极小多项式

定义2.7. 设Ω是域K的扩张，$\alpha \in \Omega$，若存在一个$K[x]$上的非零多项式$f(x)$，使得$f(\alpha)=0$，则称α是K上的**代数元**，否则称α是K上的**超越元**。

设Ω是域K的扩域，$\alpha \in \Omega$，$f(x) \in K[x]$，$degf = m$，根据定理2.5，令$Im\rho = \{g(\alpha) \mid g(x) \in K[x]\} = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \mid a_i \in K, i = 0, 1, \cdots, m-1\}$。$Im\rho$是$\Omega$的一个子域，且它同构于$K[x]/(f(x))$。令$K(\alpha) = Im\rho$，记$K(\alpha)$为最小的包含$K$，$\alpha$的$\Omega$子域，或者说$K(\alpha)$是所有包含$K$，$\alpha$的$\Omega$子域的交。

若α是数域K上的代数元，令$I = \{g(x) \in K[x]) \mid g(\alpha) = 0\}$。

设$p(x)$是I中次数最小的首1的非零多项式，且$p(x)$不可约，则$p(x)$可以整除I中任意元素。

事实上，若$f(x) = p(x)q(x) + r(x)$，则$f(\alpha) = p(\alpha)q(\alpha) + r(\alpha)$，可得$r(\alpha) = 0$，故$r(x) \in I$。又因为$degr < degp$，且$p(x)$不可约。所以$r(x) = 0$。

我们把这样的$p(x)$叫做α的**极小多项式**。

那么由定理2.5可知，$K[x]/(f(x))$与$K(\alpha)$之间存在一个域同态，且它是同构，即$K[x]/(f(x)) \cong K(\alpha)$。我们知道，扩域可以看成原来域上的线性空间，$K[x]/(f(x))$与$K(\alpha)$都可以看成$K$上的线性空间，而同构的线性空间的维数是相等的。所以$K(\alpha)$作为K上的线性空间，维数为$degp$。

定理2.8. 若$[\Omega : K]$有限，则$\forall \alpha \in \Omega$，$\alpha$是代数元。

证：$K \subseteq K(\alpha) \subseteq \Omega$，若$[\Omega : K]$有限，由维数公式可知，$[K(\alpha) : K]$也有限，而$degp = [K(\alpha) : K]$，其中$p(x)$为$\alpha$的极小多项式，即$p(\alpha) = 0$。所以$\alpha$是代数元。

2.5 尺规作图

已知有s个点$P_1(x_1, y_1)$，$\cdots$，$P_s(x_s, y_s)$。通过直尺和圆规想要得到一个新的点$P_{s+1}(x_{s+1}, y_{s+1})$。$P_{s+1}$只能通过三种方式得到：

1. 直线与直线相交

2. 直线与圆相交

3. 圆与圆相交

我们利用这些点的坐标得到一个新的域$K = Q(x_1, \cdots, x_s, y_1, \cdots, y_s)$。则$K \subseteq K(x_{s+1}, y_{s+1}) \subseteq R$。下面考虑$P_{s+1}$产生的三种情况。

1.直线与直线相交

x_{s+1}与y_{s+1}应该满足方程组

$$\begin{cases} ax + by + c = 0 \\ a'x + b'y + c' = 0 \end{cases}$$

则x_{s+1}, y_{s+1}均可由K中元素线性表出，故$x_{s+1}, y_{s+1} \in K$，即$K(x_{s+1}, y_{s+1}) = K$。

2.直线与圆相交

可由方程组

$$\begin{cases} ax + by + c = 0 \\ x^2 + y^2 + dx + ey + f = 0 \end{cases}$$

解出x_{s+1}, y_{s+1}。

将方程组消元可得

$$m_1 y^2 + m_2 y + m_3 = 0$$

可解出y_{s+1}，而x_{s+1}可通过直线方程由y_{s+1}表示。

故$K(x_{s+1}, y_{s+1}) = K(y_{s+1})$。$[K(y_{s+1}) : K] = degp$，$p(x)$为$y_{s+1}$的极小多项式，且$degp = 1$或2。

3.圆与圆相交

x_{s+1}与y_{s+1}可由下面方程组解出

$$\begin{cases} x^2 + y^2 + dx + ey + f = 0 \\ x^2 + y^2 + d'x + e'y + f' = 0 \end{cases}$$

将方程组的两式相减，即可得到与第二种情况相同类型的方程组，所以第三种情况可转化为第二种。

综上所述，$[K(x_{s+1}, y_{s+1}) : K] = 1$或2。

假如已知平面上两点$P_1(0,0)$，$P_2(0,1)$。通过一系列尺规作图可得到$P_3(x_3,y_3)$，$P_4(x_4,y_4)$，$\cdots$，$P_n(x_n,y_n)$。则对应于域扩张为

$$Q\subseteq Q(x_3,y_3)\subseteq E_1(x_4,y_4)\subseteq\cdots\subseteq E_{n-3}(x_n,y_n)$$

其中$E_0=Q$，$E_1=Q(x_3,y_3)$，$E_{i+1}=E_i(x_{i+3},y_{i+3})$，$1\leq i\leq n-3$。

则$[E_i:E_{i-1}]=1$或2。即$[E_{n-2}:Q]=2^s$。

例：证明60°度角不能用尺规三等分，即不能做出20°角。

已知$P_1(0,0)$，$P_2(0,1)$，若能得到20°角，则能得到点$P(cos20^\circ,sin20^\circ)$。则存在扩域链

$$Q\subseteq E_1\subseteq E_2\subseteq\cdots\subseteq E_{n-2}$$

使$cos20^\circ\in E_{n-2}$，且$[E_i:E_{i-1}]=1$或2。

则存在

$$Q\subseteq Q(cos20^\circ)\subseteq E_{n-2}$$

使

$$\begin{aligned}2^s &= [E_{n-2}:Q]\\ &= [E_{n-2}:Q(cos20^\circ)][Q(cos20^\circ):Q]\end{aligned}$$

$[Q(\alpha):Q]$为α在Q上的极小多项式的次数。

$cos20^\circ$在Q上的极小多项式不容易直接确定，我们可以找到它的零化多项式，极小多项式一定是零化多项式的因式。由三倍角公式可得

$$cos60^\circ=4cos^3 20^\circ-3cos20^\circ$$

则$f(x)=4x^3-3x-\frac{1}{2}$为$cos20^\circ$ 的零化多项式。而$f(x)$在Q上不可约，故$cos20^\circ$的极小多项式的次数为3。

由维数公式可知

$$2^t=[E_{n-2}:Q(cos20^\circ)]\cdot 3$$

而

$$3\nmid 2^t$$

所以不存在这样的扩域链，即通过有限次尺规作图画不出20°角。

若$K\subseteq E$为2次扩张，即$[E:K]=2$。任取$\alpha\in E$，且$\alpha\notin K$，有$K\subsetneqq K(\alpha)\subseteq E$，有维数公式可知，$[K(\alpha):K]=2$，$[E:K(\alpha)]=1$，则$E=K(\alpha)$。所以$\alpha$在$K$上的极小多项式为$x^2+ax+b\in K[x]$，而$x^2+ax+b=0$可整理为$y^2-c=0$的形式，容易求得原方程的解，解里含有平方根，那么这样的二次扩张是可以用尺规做出来的。

通过尺规我们可以等分线段、做线段倍长等长度的加减乘除运算，用尺规还可以根据射影定理进行开平方根的运算。

例如：用尺规作正五边形，就是要作出72° 角。通过计算可以得到$cos 72^\circ = \frac{\sqrt{5}-1}{4}$。用尺规进行开方、减法、除法就能得到$cos 72^\circ$。也就可以作出正五边形了。正17边形也可以这样得到，只是过程会更复杂一点，但是方法是一样的。

$$
\begin{aligned}
cos\frac{2\pi}{17} &= -\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}} \\
&+ \frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}
\end{aligned}
$$

3 分裂域

定义3.1. K是一个域，$f(x)$是$K[x]$中次数$\geq$ 1的多项式，称K的扩域E为$f(x)$的**分裂域**，如果$f(x)$在E上能够分解成一次因式的乘积，即

$$f(x) = c(x-\alpha_1)\cdots(x-\alpha_n), \alpha_i \in E$$

且$E = K(\alpha_1, \cdots, \alpha_n)$。

引理3.2. 若L，M是K上的扩域，且$\rho : M \to L$是$K-$同态。$M(\alpha)$是M上的单代数扩张。α的极小多项式为

$$p(x) = a_n x^n + \cdots a_1 x + a_0 \in M[x]$$

记

$$\rho(p(x)) = \rho(a_n)x^n + \cdots \rho(a_1)x + \rho(a_0) \in L[x]$$

若L中有$\rho(p(x))$的根β，则存在$\bar{\rho} : M(\alpha) \longrightarrow L$是一个$K-$同态，使$\bar{\rho}(m) = \rho(m)$，$\bar{\rho}(\alpha) = \beta$，且$\bar{\rho}|_M = \rho$。

注3.3. $K-$同态$\bar{\rho}$是把α映射到$\rho(p(x))$在L中的根，那么有几个根就有几个$K-$同态。

引理3.4. 若$E = K(\alpha_1, \cdots, \alpha_n)$是关于$f(x)$的一个分裂域，$L \supseteq K$是$K$的一个扩域且包含$f(x)$的所有根，则存在一个$K-$同态$\rho : E \longrightarrow L$。

证：由引理3.2可知，存在$K(\alpha_1)$到L的$K-$同态$\rho_1 : K(\alpha_1) \longrightarrow L$。$K(\alpha_1)(\alpha_2)$是$K(\alpha_1)$ 上的单代数扩张，设α_2在$K(\alpha_1)$ 上的极小多项式为$p_2(x)$，由于α_2为$f(x)$的根，所以$p_2(x)$为$f(x)$的因式。故$\rho(p_2(x))$在L中一定有根β，由引理3.2，存在$K-$同态$\rho_2 : K(\alpha_1)(\alpha_2) \longrightarrow L$，使得$\rho_2(\alpha_2) = \beta$。同理，存在$K-$同态$\rho_3 : K(\alpha_1, \alpha_2)(\alpha_3) \longrightarrow L$。以此类推，存在$E$到$L$的一个$K-$同态。

定理3.5. 域K上的多项式$f(x)$的分裂域存在，且在同构意义下是唯一的。

证：先证存在性。$f(x)$的分裂域是显然存在的。如果$f(x)$的有些根不在K上，我们可以找到这些根的极小多项式，构造干域来找那些根，最多做$degf$ 次代数扩张，就一定可以找到$f(x)$的所有根。

再证唯一性。若E_1，E_2是$f(x)$的两个分裂域，由引理3.4，存在$K-$同态$\rho_1 : E_1 \longrightarrow E_2$ 和$\rho_2 : E_2 \longrightarrow E_1$，由于$K-$同态是域同态，一定是单射。$E_1$，$E_2$作为$K$上的线性空间，由两个$K-$同态可知，$dimE_1 \leq dimE_2 < \infty$且$dimE_2 \leq dimE_1 < \infty$，则$dimE_1 = dimE_2$，即$E_1 \cong E_2$。证毕

设$K(\alpha_1, \cdots, \alpha_n)$为$f(x)$的分裂域，$L$为$K$的扩域，且包含$f(x)$的所有根。

$$\begin{tikzcd}
K \arrow[d, "\rho_0"'] & \subseteq & K(\alpha_1) \arrow[dll, "\rho_1"'] & \subseteq & K(\alpha_1,\alpha_2) \arrow[dllll, "\rho_2"'] & \subseteq & \cdots & \subseteq & K(\alpha_1,\cdots,\alpha_n) \arrow[dllllllll, "\rho_n"'] \\
L
\end{tikzcd}$$

$\rho_0 = id$，$\rho_{i+1}|_{K(\alpha_1,\cdots,\alpha_i)} = \rho_i$。

给定ρ_i，ρ_{i+1}的选择可能性个数就是$\rho_i(p_{i+1}(x))$在L上的不同的根的个数，其中$p_{i+1}(x)$为α_{i+1}在$K(\alpha_1, \cdots, \alpha_i)$中的极小多项式。$[K(\alpha_1, \cdots, \alpha_i)(\alpha_{i+1}) : K(\alpha_1, \cdots, \alpha_i)] = degp_{i+1}$，所以$\rho_n$的可能个数$\leq [K(\alpha_1, \cdots, \alpha_n) : K] \leq n!$。当有重根的时候就会小于$n!$，当$K$的特征为0或$f(x)$没有重根是取等号。

例：$f(x) = x^3 - 2$在Q上不可约，在C上有三个根。

$$\begin{tikzcd}
Q \arrow[d, "id"'] & \subseteq & Q(\sqrt[3]{2}) \arrow[dll, "\rho_1"'] & \subseteq & Q(\sqrt[3]{2})(\sqrt[3]{2}\omega) \arrow[dllll, "\rho_2"'] & \subseteq & Q(\sqrt[3]{2},\sqrt[3]{2}\omega)(\sqrt[3]{2}\omega^2) \arrow[dllllll, "\rho_3"'] \\
C
\end{tikzcd}$$

因为$\sqrt[3]{2}$在Q上的极小多项式为$p_1(x) = x^3 - 2$。它在C上有三个根，所以ρ_1有三种选择。

假设$\rho_1 : \sqrt[3]{2} \longrightarrow \sqrt[3]{2}\omega$，$\sqrt[3]{2}\omega$的一个零化多项式为$p_2(x) = \frac{x^3-2}{x-\sqrt[3]{2}} = x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2$，而$p_2(x)$的判别式小于零，在实数域上是不可约的，所以在实数域的子域$Q(\sqrt[3]{2})$上也是不可约的，即$p_2(x)$为$\sqrt[3]{2}\omega$在$Q(\sqrt[3]{2})$上的极小多项式，那么

$$\rho_1(p_2(x)) = x^2 + \sqrt[3]{2}\omega x + (\sqrt[3]{2}\omega)^2$$

$\rho_1(p_2(x))$在复数域上有两个根$\sqrt[3]{2}$和$\sqrt[3]{2}\omega^2$，所以ρ_2有两种选择。

再假设$\rho_2 : \sqrt[3]{2}\omega \longrightarrow \sqrt[3]{2}\omega^2$，那么$\rho_3$就应该是$\rho_3 : \sqrt[3]{2}\omega^2 \longrightarrow \sqrt[3]{2}$。事实上，当确定了$\rho_1$和$\rho_2$，也就确定了$\sqrt[3]{2}$和$\omega$的像，那么$\rho_3$就可以直接给

出，或者说ρ_1和ρ_2都是ρ_3的限制，由于同态保持运算

$$\rho_3(\sqrt[3]{2}\omega^2) = \rho_3(\frac{(\sqrt[3]{2}\omega)^2}{\sqrt[3]{2}}) = \frac{\rho_2((\sqrt[3]{2}\omega)^2)}{\rho_1(\sqrt[3]{2})} = \sqrt[3]{2}$$

最后我们会得到6个ρ_3。

4 Galois基本定理

4.1 自同构群

定义4.1. E/K是域扩张（K的特征数为0，$E = K(\alpha_1, \cdots, \alpha_s)$是有限代数扩张），若$\rho : E \longrightarrow E$是$K-$同态，称$\rho$是$E$的$K-$**同构**。

所有$K-$同构做成的集合在映射复合运算下构成一个群，称为E的**自同构群**，记作$Aut(E/K)$。

例：$E = Q(\sqrt[3]{2})$，$\sqrt[3]{2}$在Q上的极小多项式在E上只有一个根$\sqrt[3]{2}$。所以E 的自同构群是平凡的，只有id。

例：$E = Q(\sqrt{2})$，$\sqrt{2}$在Q上的极小多项式在E上有两个根，则E的自同构群中有两个元素。

例：$E = Q(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$，前面我们已经算过，它是$Q$上的不可约多项式$f(x) = x^3 - 2$的分裂域，$E$ 的自同构有6个。

$$\rho_1 : \sqrt[3]{2} \longrightarrow \sqrt[3]{2}, \sqrt[3]{2}\omega \longrightarrow \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2 \longrightarrow \sqrt[3]{2}\omega^2$$
$$\rho_2 : \sqrt[3]{2} \longrightarrow \sqrt[3]{2}, \sqrt[3]{2}\omega \longrightarrow \sqrt[3]{2}\omega^2, \sqrt[3]{2}\omega^2 \longrightarrow \sqrt[3]{2}\omega$$
$$\rho_3 : \sqrt[3]{2} \longrightarrow \sqrt[3]{2}\omega, \sqrt[3]{2}\omega \longrightarrow \sqrt[3]{2}, \sqrt[3]{2}\omega^2 \longrightarrow \sqrt[3]{2}\omega^2$$
$$\rho_4 : \sqrt[3]{2} \longrightarrow \sqrt[3]{2}\omega, \sqrt[3]{2}\omega \longrightarrow \sqrt[3]{2}\omega^2, \sqrt[3]{2}\omega^2 \longrightarrow \sqrt[3]{2}$$
$$\rho_5 : \sqrt[3]{2} \longrightarrow \sqrt[3]{2}\omega^2, \sqrt[3]{2}\omega \longrightarrow \sqrt[3]{2}, \sqrt[3]{2}\omega^2 \longrightarrow \sqrt[3]{2}\omega$$
$$\rho_6 : \sqrt[3]{2} \longrightarrow \sqrt[3]{2}\omega^2, \sqrt[3]{2}\omega \longrightarrow \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2 \longrightarrow \sqrt[3]{2}$$

如果把$\sqrt[3]{2}$，$\sqrt[3]{2}\omega$，$\sqrt[3]{2}\omega^2$分别记为1，2，3。那么这些同构可以看作是根之间的对应。

$$\rho_1 : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1), \quad \rho_2 : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$$
$$\rho_3 : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12), \quad \rho_4 : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$$
$$\rho_5 : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132), \rho_6 : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$$

所以E的自同构群同构于6阶置换群S_3。

引理4.2. $[E : K]$有限，则$[E : K] \geq |Aut(E/K)|$。

当E是K上关于多项式$f(x)$的分裂域时，等号成立。

引理4.3. E是一个域，$G \triangleq \{\rho_i|\rho_i$是$E$到$E$的域同构$, i = 1, \cdots, n\}$，且$G$在映射复合意义下构成一个群。$E^G = K \triangleq \{x \in E|\rho_i(x) = x, i = 1, \cdots, n\}$称为稳定子域，则$[E:K] \leq |G|$。（$|G|$ 有限时，等号成立。）

证：任取$\alpha_1, \cdots, \alpha_m \in E(m > n)$，下证存在$x_1, \cdots, x_m \in K$不全为0，使得$x_1\alpha_1 + \cdots + x_m\alpha_m = 0$。

考虑方程组$x_1\rho_i(\alpha_1) + \cdots + x_m\rho_i(\alpha_m) = 0. i = 1, 2, \cdots, n$。因为未知数个数大于方程个数，所以方程组在$E$上有非零解。注意到方程组在$E$中的解有如下性质：

1. 解构成一个线性空间W。
2. $x = (a_1, \cdots, a_m) \in W$，则$(\rho_j(a_1), \cdots, \rho_j(a_m)) \in W, j = 1, \cdots, n$。

性质1显然成立，对于性质2

$$a_1\rho_i(\alpha_1) + \cdots + a_m\rho_i(\alpha_m) = 0$$

$$\rho_j(a_1)\rho_j\rho_i(\alpha_1) + \cdots + \rho_j(a_m)\rho_j\rho_i(\alpha_m) = 0$$

因为ρ_i是E的自同构，所以$\rho_j\rho_i(\alpha_1), \cdots, \rho_j\rho_i(\alpha_m)$是$\alpha_1, \cdots, \alpha_m$的一个排列，一定存在$\rho_k = \rho_j\rho_i$，使

$$\rho_j(a_1)\rho_k(\alpha_1) + \cdots + \rho_j(a_m)\rho_k(\alpha_m) = 0$$

由于群G的运算封闭，当i取遍1到n时，k也能取遍1到n。即$(\rho_j(a_1), \cdots, \rho_j(a_m))$也是方程组的解。

取$x_1\alpha_1 + \cdots + x_m\alpha_m = 0$在$E$上的一个非零解$x_0 = (a_1, \cdots, a_m) \in W_0$。若$a_1 \in K$，则判断$a_2$，若$a_1 \notin K$，用$a_1$的逆元素把$a_1$变成1；若$a_2 \in K$，则判断$a_3$，若$a_2 \notin K$，则存在$\rho_t(a_2) \neq a_2$，令$x_0' = x_0 - \rho_t(x_0) = (0, a_2', \cdots, a_m')$。若$a_2' \notin K$，把$a_2'$变成1，这样依次进行下去，最后得到的$\bar{x}_0 \in K$（注：$0, 1 \in K$）。

综上，存在$x_1, \cdots, x_m \in K$不全为0，使得$x_1\alpha_1 + \cdots + x_m\alpha_m = 0$。即任意大于$n$个元素都是线性相关的，所以$[E:K] \leq |G|$。

推论4.4. 若$\alpha_1, \cdots, \alpha_n$是$E/K$的一组基，则

$$\det\begin{pmatrix} \rho_1(\alpha_1) & \rho_1(\alpha_2) & \cdots & \rho_1(\alpha_n) \\ \rho_2(\alpha_1) & \rho_2(\alpha_2) & \cdots & \rho_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \rho_n(\alpha_1) & \rho_n(\alpha_2) & \cdots & \rho_n(\alpha_n) \end{pmatrix} \neq 0$$

4.2 Galois基本定理

定义4.5. 设K是一个域，E/K是有限扩张，若K是E的$K-$自同构群的稳定子域，即$K = E^{Aut(E/K)}$，则称E/K为**Galois扩张**。这时群$Aut(E/K)$叫做**Galois群**，记作$Gal(E/K)$。

定义4.6. 设E是K的一个有限扩张，如果K上的一个不可约多项式在E中有一个根时，它在E上就能完全分解成一次因式的乘积，则称E是K 的**正规扩张**。

定理4.7. 域K的特征是0，E/K是有限扩张，则以下叙述等价：

(1) E是K上关于$f(x)$的分裂域。

(2) E/K是Galois扩张。

(3) E是K上的正规扩张。

推论4.8. $K \subseteq M \subseteq E$为域扩张。若$E/K$是Galois扩张，则$E/M$也是Galois扩张。

证：由定理4.7可知，E为K上的某个多项式$f(x)$的分裂域，因为M为K的扩域，作为M上的多项式，$f(x)$在E上也能分解成一次因式的乘积，即E为M上$f(x)$的分裂域，则E/M是Galois扩张。

推论4.9. 域K的特征是0，E/K是有限扩张，总是存在一个K上的分裂域L，使得$K \subseteq E \subseteq L$。

证：令$E = K(\alpha_1, \cdots, \alpha_m)$。$\alpha_i$ 在K上的极小多项式为$f_i(x)$，取L为K上关于$\prod\limits_{i=1}^{m} f_i(x)$的分裂域，显然$L$为$K$的扩域。

定理4.10. （Galois基本定理）设E/K是Galois 扩张

(1) $K \subseteq M \subseteq E$，$M$为中间域，则存在映射$\rho : M \longmapsto Gal(E/M)$，其中$Gal(E/M)$为$Gal(E/K)$的子群。

(2) H为$Gal(E/K)$的子群，则E^H是中间域，即存在映射$\sigma : H \longmapsto E^H$，使$K \subseteq E^H \subseteq E$。

(3) ρ与σ互逆。

(4) $K \subseteq M \subseteq E$，$M/K$是Galois扩张$\Longleftrightarrow Gal(E/M) \lhd Gal(E/K)$，且$Gal(M/K) \cong Gal(E/K)/Gal(E/M)$。

证：这里先不给出(4)的证明。

(1) M为中间域，由推论4.8，E/M也为Galois 扩张，即有$M = E^{Gal(E/M)}$。

(2) $H \subseteq Gal(E/K) \Longrightarrow E^{Gal(E/K)} \subseteq E^H$，而$E^{Gal(E/K)} = K$，所以$E^H$为$K \subseteq E$ 的中间域。

(3) $\sigma\rho : M \longmapsto H = Gal(E/M) \longmapsto E^H$，往证$M = E^H$。显然有$M \subseteq E^H$，对于域扩张$K \subseteq M \subseteq E^H \subseteq E$，$H = Gal(E/E^H)$，已知$H = Gal(E/M)$，则$M \subseteq E^H$为一次扩张，即$M = E^H$。

$\rho\sigma : H \longmapsto M = E^H \longmapsto Gal(E/M)$，而$H = Gal(E/E^H) = Gal(E/M)$。

故$\sigma\rho = \rho\sigma = 1$。

命题4.11. E/K是有限扩张，K的特征是0，则存在$\alpha \in E$，使$E = K(\alpha)$。

证：由Galois基本定理可知，Galois扩张的中间域与Galois群的子群之间有一一对应的关系。若E/K不是Galois扩张，由推论4.9，存在一个分裂域L使L/K为Galois扩张，$Gal(E/K)$是有限群，则$L \supseteq K$的中间域为有限个，而K作为L的子域，$E \supseteq K$的中间域也为有限个。

设$M_i(i = 1, \cdots, m)$为$E \supseteq K$的所有中间域，M_i与E作为K上的线性空间，有$\bigcup\limits_{i=1}^{m} M_i \neq E$，存在$\alpha \in E$且$\alpha \notin M_i$，故$E = K(\alpha)$。因为$K(\alpha) \neq K$，且$K(\alpha)$不等于所有的中间域。

5 有限群

5.1 群

定义5.1. 一个非空集合G与G上的一个叫做乘法的二元运算"$\cdot$"，假如：

(1) G对乘法运算是封闭的，即$\forall a, b \in G$，$a \cdot b \in G$，

(2) 乘法"$\cdot$"满足结合律，即对于$\forall a, b, c \in G$，$(a \cdot b) \cdot c = a \cdot (b \cdot c)$，

(3) 有单位元e，即$\forall a \in G$，$a \cdot e = e \cdot a = a$，

(4) 有逆元，即$\forall a \in G$，$\exists b \in G$，使$a \cdot b = b \cdot a = e$，

则称$(G, \cdot)$为**群**。

集合X上所有双射构成的集合，在映射复合运算下构成一个群，若X中含有n个元素，我们记这个群为S_n，称为置换群。

定义5.2. 我们称群G所含元素的个数为**群G的阶**，记为$|G|$。若$|G| = n < +\infty$，称G是n阶有限群，否则称G为无限群。

显然，$|S_n| = n!$。

定义5.3. $\forall a \in G$，使得$a^m = e$的最小正整数m叫做**元素a的阶**。

规定单位元的阶为0。

定义5.4. 群G的一个子集H叫做G的一个**子群**，假如H对于G的运算做成一个群。

H是G的子群，若$\alpha \in H$，则$\alpha^i \in H$，且$\{e, \alpha^{\pm 1}, \alpha^{\pm 2}, \cdots\}$是$G$中包含$\alpha$的最小子群。$\alpha$的阶等于由$\alpha$生成的子群$< a >$的阶。

5.2 正规子群与商群

我们看一个群G和群G的一个子群H，规定一个G 中元素之间的关系$\sim$：

$$a \sim b\text{，当且仅当}ab^{-1} \in H$$

1. $aa^{-1}=e\in H$，所以

$$a\sim a$$

2. $ab^{-1}\in H\Rightarrow(ab^{-1})^{-1}=ba^{-1}\in H$，所以

$$a\sim b\Rightarrow b\sim a$$

3. $ab^{-1}\in H,bc^{-1}\in H\Rightarrow(ab^{-1})(bc^{-1})=ac^{-1}\in H$，所以

$$a\sim b,b\sim c\Rightarrow a\sim c$$

这样可知，$\sim$是一个等价关系。利用这个等价关系，我们可以得到G的一个分类。

定义5.5. 由等价关系$\sim$决定的类叫做子群H的**右陪集**。包含元素a的右陪集用Ha表示。

例：$G=S_3=\{(1),(12),(13),(23),(123),(132)\}$，$H=\{(1),(12)\}$ 那么

$$H(1)=\{(1),(12)\}$$
$$H(13)=\{(13),(123)\}$$
$$H(23)=\{(23),(132)\}$$

子群H把群G分成$H(1)$，$H(13)$，$H(23)$三个不同的右陪集。

假如我们定义的关系为$\sim'$：

$$a\sim' b\text{，当且仅当}b^{-1}a\in H$$

那么$\sim'$也是一个等价关系，也决定了一个群G的分类。

定义5.6. 由等价关系$\sim'$ 决定的类叫做子群H的**左陪集**。包含元素a的左陪集用aH表示。

例：前面例题中H的左陪集为

$$(1)H=\{(1),(12)\}$$
$$(13)H=\{(13),(132)\}$$
$$(23)H=\{(23),(123)\}$$

可以看出H的左右陪集是不相同的。

同一子群的陪集可能不相同，但是左右陪集的个数一定是相等的。

定义5.7. 群G的一个子群H的右陪集（或左陪集）的个数叫做H在G里的**指数**，记作$|G:H|$。

那么我们会有以下定理。

定理5.8. （Lagrange定理）设G是有限群，H是G的子群。则

$$|G| = |G : H||H|$$

推论5.9. 有限群G的任一元素a的阶n都能整除G的阶。

证：阶为n的元素会生成一个n阶子群，由Lagrange 定理，n可以整除G的阶。

定义5.10. 设H是群G的子群，若对$\forall a \in G$都有$aH = Ha$，则称H是G的**正规子群**，记作$H \lhd G$。

例：G与$\{e\}$是群G的正规子群，它们是平凡的正规子群。

定义5.11. 如果群G的正规子群只有G和$\{e\}$，则称G为**单群**。

注5.12. 所谓$aH = Ha$，并不是说a可以和H 的每一个元素可交换，而是aH和Ha这两个集合一样。

定理5.13. 设H是群G的子群，则下列条件等价：

(1) H是G的正规子群，

(2) $gHg^{-1} = H$，$\forall g \in G$，

(3) $gHg^{-1} \subseteq H$，$\forall g \in G$，

(4) $ghg^{-1} \in H$，$\forall g \in G$，$\forall h \in H$。

例：交换群的子群都是正规子群。

例：与群G所有元素可交换的元素组成的集合$C(G)$，叫做群G的中心。$C(G)$是G的正规子群。

设H是群G的一个正规子群，把H的陪集做成一个集合

$$\{aH, bH, cH, \cdots\}$$

规定运算，$\forall x, y \in G$，$(xH)(yH) = (xy)H$。

下面验证运算定义的合理性，即运算结果与代表元素x, y的选择无关。

若

$$xH = x'H，yH = y'H$$

那么

$$x = x'h_1，y = y'h_2，(h_1, h_2 \in H)$$

$$xy = x'h_1y'h_2$$

由于H是正规子群，

$$h_1y' \in Hy' = y'H$$
$$h_1y' = y'h_3, (h_3 \in H)$$

则

$$xy = x'y'(h_3h_2)$$
$$xy \in x'y'H$$

所以

$$xyH = x'y'H$$

H的陪集构成的集合在上述运算下构成一个群。

(1) 运算封闭性显然。

(2) $\forall x, y, z \in G$，

$$(xHyH)zH = (xy)HzH = (xyz)H$$
$$xH(yHzH) = xH(yz)H = (xyz)H$$

(3) $eHxH = xHeH = xH$

(4) $(x^{-1})HxH = (x^{-1}x)H = eH$

定义5.14. 群G的一个正规子群H的陪集所做成的群叫做G关于H的**商群**，记作G/H。

定理5.15. 群同态基本定理：

(1) $N \lhd G$，则$\pi : G \longrightarrow G/N (\pi : h \longmapsto hN)$是群同态。

(2) $\rho : G \longrightarrow H$是群同态，则$ker\rho \lhd G$，且$G/ker\rho \cong Im\rho$，即存在唯一的$\bar{\rho} : G/ker\rho \longrightarrow Im\rho$，使得$\rho = \bar{\rho} \circ \pi$。

$$\begin{tikzcd}
G \arrow[r, "\rho"] \arrow[d, "\pi"'] & Im\rho & \subseteq & H \\
G/ker\rho \arrow[ur, "\bar{\rho}"'] & & &
\end{tikzcd}$$

(3) $N \lhd G$，则G/N的子群与N，G的中间子群一一对应，且正规子群与正规子群对应。

证：(1) 显然π是一个很自然的同态。

(2) 先证$ker\rho$是G的正规子群。$\forall a, b \in ker\rho$，$\rho(ab^{-1}) = \rho(a)\rho(b^{-1}) = e_He_H^{-1} = e_H$，$ab^{-1} \in ker\rho$，所以$ker\rho$是$G$的一个子群。$\forall a \in ker\rho$，$\forall g \in G$，$\rho(gag^{-1}) = \rho(g)e_H\rho(g^{-1}) = \rho(gg^{-1}) = e_H$，则$gag^{-1} \in ker\rho$，那么$ker\rho$就是$G$的正规子群。

定义$\bar{\rho}: g \cdot ker\rho \longmapsto \rho(g)$。

首先，对$\forall x, y \in G$，若$x \cdot ker\rho = y \cdot ker\rho$，$\exists h \in ker\rho$，使$x = yh$。那么$\rho(x) = \rho(yh) = \rho(y)\rho(h) = \rho(y) \cdot e_H = \rho(y)$，即$\bar{\rho}(x \cdot ker\rho) = \bar{\rho}(y \cdot ker\rho)$，所以$\bar{\rho}$是$G/ker\rho$到$H$的映射。

其次，$\forall x, y \in G$，$\bar{\rho}(xker\rho \cdot yker\rho) = \bar{\rho}(xyker\rho) = \rho(xy) = \rho(x)\rho(y) = \bar{\rho}(xker\rho)\bar{\rho}(yker\rho)$。所以$\bar{\rho}$是群同态。

然后，$\forall x \cdot ker\rho \in ker\bar{\rho}$，$e_H = \bar{\rho}(xker\rho) = \rho(x)$，则$x \in ker\rho$，即$xker\rho = ker\rho$是商群$G/ker\rho$的单位元，这就是说，$\bar{\rho}$是单同态，所以$\bar{\rho}$是同构。

最后，$\forall g \in G$，$\bar{\rho}\pi(g) = \bar{\rho}(gker\rho) = \rho(g)$，即$\bar{\rho}\pi = \rho$。

循环群结构定理

设G是一个群，$\forall g \in G$，$< g >= \{e, g^{\pm 1}, g^{\pm 2}, \cdots\}$。

定义5.16. 若$\exists g \in G$，使$G =< g >$，则称G为**循环群**。

循环群$G =< g >$与整数群Z之间存在自然同态ρ，使$\rho(n) = g^n$，$n \in Z$。由同态基本定理，

$$Z/ker\rho \cong Im\rho = G$$

即循环群同构于整数群的商群。

当G是无限群时，$ker\rho = \{0\}$，即$G \cong Z$。当G是有限群时，$\exists n \in Z^+$，使$g^n = e$，$ker\rho = \{nZ | n \in Z^+\}$，则$G \cong Z/nZ$。

整数群Z的所有子群都形如$\{nZ | n \in Z^+\}$。事实上，若H是Z的子群，取H中最小正整数a，则aZ是Z的子群，若存在$b \in H$且$b \notin aZ$，有$b = ka + r$，$0 < r < a$，与a是H中最小正整数矛盾。

设G是n阶循环群，则$G \cong Z/nZ$。由同态基本定理，G的子群与Z中包含aZ的子群一一对应。若$n'Z$为Z中包含nZ的子群，则$n' | n$。所以，对$\forall d | n$，G的d 阶子群存在，而且只有一个。

下面我们来看一下S_n。

$S_n = \{\sigma | \sigma$是$\{1, 2, \cdots, n\}$上的双射$\}$。$\forall \sigma, \tau \in S_n$，$\sigma\tau(x) \triangleq \sigma(\tau(x))$。

S_n中的元素有三种表示：

1. 置换表示

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

2. 轮换表示：$(i_1i_2\cdots i_t)(j_1j_2\cdots j_s)\cdots$

$\sigma(i_k)=i_{k+1}$，$1\le k\le t-1$，$\sigma(i_t)=i_1$，$\sigma(j_k)=j_{k+1}$，$1\le k\le s-1$，$\sigma(j_s)=j_1$等等

3. 对换表示

S_n中每一个元素σ都可以写成若干个对换的合成。若有奇数个对换，称σ为奇置换；若有偶数个对换，称σ为偶置换。所有的偶置换构成一个群，叫做交错群，记作A_n。

例：$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}=(134)(25)=(14)(13)(25).$

定义5.17. 群G中的两个元素a,b**共轭**，如果存在G中的元素g，满足$gag^{-1}=b$。

群G中元素的共轭关系是一个等价关系，决定了G的一个分类，所有与g共轭的元素构成g的共轭类。

命题5.18. 设$\sigma=(a_1a_2\cdots a_t)\in S_n$，对$\forall\tau\in S_n$，有

$$\tau\sigma\tau^{-1}=(\tau(a_1)\tau(a_2)\cdots\tau(a_t))$$

证：若$1\le j<t$，$\tau\sigma\tau^{-1}(\tau(a_j))=\tau\sigma(a_j)=\tau(a_{j+1})$，$\tau\sigma\tau^{-1}(\tau(a_t))=\tau\sigma(a_t)=\tau(a_1)$。若$l\in\{1,2,\cdots,n\}\backslash\{\tau(a_1),\tau(a_2),\cdots,\tau(a_t)\}$，$\tau^{-1}(l)\notin\{a_1,a_2,\cdots,a_t\}$，$\tau\sigma\tau^{-1}(l)=\tau\sigma(\tau^{-1}(l))=\tau\tau^{-1}(l)=l$。

推论5.19. $\forall g,h\in S_n$，g与h共轭$\Longleftrightarrow$ g与h的轮换类型一致。

由定理5.13可知，正规子群一定是若干共轭类的并。

S_3只有6个元素，3个共轭类，它的非平凡正规子群只有$A_3=\{(1),(123),(132)\}$。

S_4的情况稍复杂一点，它有24个元素，5个共轭类，

$$\begin{cases}(1)\\(12),(13),(14),(23),(24),(34)\\(123),(124),(134),(234),(132),(142),(143),(243)\\(1234),(1243),(1324),(1342),(1423),(1432)\\(12)(34),(13)(24),(14)(23)\end{cases}$$

S_4的非平凡正规子群的阶一定是24的因子，而且正规子群中一定含有(1)，根据群的阶就能排除很多共轭类的组合情况。经验证，S_4的非平

凡正规子群只有4阶的和12阶的。

$$K_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$$

$$\begin{aligned} A_4 =& \{(1), (12)(34), (13)(24), (14)(23), (123), (124), \\ & (134), (234), (132), (142), (143), (243)\} \end{aligned}$$

那么在S_4，S_3之间存在满同态$f : S_4 \longrightarrow S_3$

$$S_4/kerf \cong S_3$$

则$kerf = K_4$。

商群S_4/K_4中的元素为：

$$\begin{cases} (1)K_4 = \{(1), (12)(34), (13)(24), (14)(23)\} \\ (12)K_4 = \{(12), (34), (1423), (1324)\} \\ (13)K_4 = \{(13), (24), (1432), (1234)\} \\ (23)K_4 = \{(23), (14), (1243), (1342)\} \\ (123)K_4 = \{(123), (243), (142), (134)\} \\ (132)K_4 = \{(132), (234), (124), (143)\} \end{cases}$$

那么$f : aK_4 \longrightarrow a$，显然是一个$S_4$到$S_3$的满同态。

命题5.20. $A_n (n \geq 5)$的单群。

证：我们要证明A_n是单群，需要证明若$\{(1)\} \neq N \lhd A_n$，则$N = A_n$。

(1) A_n可由所有3轮换生成。设$(1) \neq \sigma \in A_n$，因为σ是偶置换，σ 可写成偶数个对换的乘积，对于任意两个不同的对换乘积，我们有

$$(ij)(jk) = (ijk)$$

$$(ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl)$$

所以σ可以表示成若干3轮换的乘积。

(2) 设$(1) \neq \sigma \in N$是N中变动$\{1, 2, \cdots, n\}$中元素最少的元素，则σ一定是3轮换。

若σ的轮换表示是2个对换的乘积。不妨设$\sigma = (12)(34)$，取$\tau = (345)$，则$\sigma^{-1}\tau\sigma\tau^{-1} = (345) \in N$，与$\sigma$的选取相矛盾。

若σ的轮换表示是更多个对换的乘积。不妨设$\sigma = (12)(34)(56)\cdots$，取$\tau = (123)$，则$\sigma^{-1}\tau\sigma\tau^{-1} = (13)(24) \in N$，与$\sigma$的选取相矛盾。

所以σ的最长轮换部分的长度≥ 3。把最长的轮换写在前面，若σ不是3轮换，则σ有如下形状：

(a) $\sigma = (123)(45)\cdots$

(b) $\sigma = (123)(456)\cdots$

(c) $\sigma = (1234\cdots)\cdots$

因为σ是偶置换，$(a)(b)$中变动的元素个数≥ 6，若个数< 6，$\sigma = (123)(45)$不是偶置换。(c)中变动元素个数≥ 5。

对于(a)，取$\tau = (234)$，则$\sigma^{-1}\tau\sigma\tau^{-1} = (12435) \in N$，与$\sigma$的选取矛盾。对于$(b)$，取$\tau = (245)$，则$\sigma^{-1}\tau\sigma\tau^{-1} = (16425) \in N$，与$\sigma$的选取矛盾。对于$(c)$，取$\tau = (243)$，则$\sigma^{-1}\tau\sigma\tau^{-1} = (134) \in N$，与$\sigma$的选取矛盾。

因此，σ一定是3轮换。

(3) N包含所有的3轮换。因为N是A_n的正规子群，所以N包含3轮换的共轭类，也就是所有的3轮换。

综上，$N = A_n$，所以A_n是单群。

命题5.21. $S_n(n \geq 5)$的非平凡正规子群只有A_n。

证：设$A_n \lhd S_n$，$M \lhd S_n$，且$M \neq \{(1)\}$或S_n，只需证明$M = A_n$。

因为$M \lhd S_n$，则$M \cap A_n \lhd A_n$，而A_n是单群，$M \cap A_n = \{(1)\}$或A_n。若$M \cap A_n = \{(1)\}$，则$M = \{(1)\}$。因为如果M中有奇置换，至少会包含奇置换的一个共轭类，任意两个元素的乘积也在M中，而两个奇置换的乘积是偶置换，则$M \cap A_n$中还会有其他元素。若$M \cap A_n = A_n$，则A_n是M的子群，$|A_n| = \frac{n!}{2}$，那么$\frac{n!}{2} \leq |M| < n!$，只能$M = A_n$。所以$S_n$的非平凡正规子群只有$A_n$。

在对群论有了一些了解之后，下面我们给出Galois基本定理中(4)的证明。

(4) $K \subseteq M \subseteq E$，$M/K$是Galois扩张$\Longleftrightarrow Gal(E/M) \lhd Gal(E/K)$，且$Gal(M/K) \cong Gal(E/K)/Gal(E/M)$。

证：" $\Longrightarrow$ " 设$H = Gal(E/M) \lhd Gal(E/K)$，则$E^H = M$，取$\alpha \in E^H$，$\alpha$在$K$ 上的极小多项式为$p(x)$，$p(x)$在E上有s个根$\alpha = x_1, \cdots, x_s$。对于$x_i(2 \leq i \leq s)$，一定存在$g \in Gal(E/K)$，使得$x_i = g(x_1)$，那么$h(x_i) = h(g(x_1))$，由于$H$为$Gal(E/K)$的正规子群，$\exists h' \in H$，使$hg =$

gh'，则$h(x_i) = hg(x_1) = g(h'(x_1)) = g(x_1) = x_i$，所以$x_i \in E^H$，即所有的根都在$E^H$中，$E^H/K$为正规扩张，由定理4.7，$E^H/K$为Galois扩张。

”$\Longleftarrow$”若M/K是Galois扩张，设$H = Gal(E/M)$。
由于M/K是Galois扩张，$\forall \alpha \in M$，M包含α 在K上的极小多项式的所有根，所以$\forall g \in G$，$g(\alpha) \in M$。$\forall h \in H$，$ghg^{-1}(\alpha) = gh(g^{-1}(\alpha)) = gg^{-1}(\alpha) = \alpha$。则$\alpha \in E^{gHg^{-1}}$，那么$M \subseteq E^{gHg^{-1}}$，而$M = E^H$，可得$gHg^{-1} \subseteq H$，所以$H$为$Gal(E/K)$的正规子群。

另外，存在一个$Gal(E/K)$到$Gal(M/K)$群同态$\rho : g \longmapsto g|_M$，由同态基本定理

$$Gal(E/K)/ker\rho \cong Im\rho$$

M是E的子域，ρ一定是满同态，则$Im\rho = Gal(M/K)$，而$ker\rho$中的元素就是在E 上保持M不动的自同构，也就是$Gal(E/M)$，所以有$Gal(M/K) \cong Gal(E/K)/Gal(E/M)$。

注5.22. 在Galois理论中，存在一个群链与域链反向的对应关系

$$\begin{array}{ccccccc}
E_0 & \subseteq & E_1 & \subseteq & \cdots & \subseteq & E \\
\downarrow & & \downarrow & & & & \downarrow \\
G_n & > & G_{n-1} & > & \cdots & > & \{id\}
\end{array}$$

越大的域对应的Galois群就越小，这是显然的事情，域对应的Galois群是保持域中元素不动的自同构，域越大，在自同构下不动的元素就越多，而这样的自同构也就越少。

6 Galois群的计算

先介绍一下群作用。

定义6.1. G是一个群，Ω是一个非空集合，群G在Ω上的一个**作用**是指G到S_Ω的一个同态。$\forall g \in G$，$\rho(g)$是Ω到Ω的双射。

定义6.2. 设群G作用在集合Ω上，则对每个$\alpha \in \Omega$，

$$G_\alpha = \{g \in G | g(\alpha) = \alpha\}$$

是G的子群，叫做α的**稳定子群**。

定义6.3. 设群G作用在集合Ω上，$x, y \in \Omega$称为**等价**的，如果存在$g \in G$，使$g(x) = y$。容易验证这是一个等价关系，每一个等价类叫做G在Ω上的一个**轨道**（传递集）。记$G(\alpha) = \{g(\alpha)|g \in G\}$为$\alpha$ 所在的轨道。如果G在Ω上只有一个轨道，则称G在Ω上的作用是**传递的**。

定理6.4. 设有限群G作用在有限集合Ω 上，$\alpha \in \Omega$，则

$$|G(\alpha)| = |G : G_\alpha|$$

证：对于$\forall g, h \in G$

$$g(\alpha) = h(\alpha) \Longleftrightarrow g^{-1}h(\alpha) = \alpha \Longleftrightarrow g^{-1}h \in G_\alpha \Longleftrightarrow hG_\alpha = gG_\alpha$$

则存在一个从G_α的左陪集集合到轨道集合的双射$f : gG_\alpha \longmapsto g(\alpha)$，所以$|G(\alpha)| = |G : G_\alpha|$。

设K是一个域，K的特征为0，$f(x) \in K[x]$，E是K上关于$f(x)$的分裂域，$G_f \triangleq G = Gal(E/K)$，为了叙述方便，假定$f(x)$没有重根。

$f(x)$在E上的n个不同的根为$\alpha_1, \cdots, \alpha_n$，$\forall g \in G_f$，$g$为$\{\alpha_1, \cdots, \alpha_n\}$上的双射，存在同态$\rho : G_f \longrightarrow S_{\{\alpha_1,\cdots,\alpha_n\}}$，则$\rho$ 是一个单同态。事实上，若$g(\alpha_i) = \alpha_i$，$\forall \alpha \in E$，α都可由$k, \alpha_1, \cdots, \alpha_n$的加减乘除运算得到，则$g(\alpha) = \alpha$，所以$g = id$。由于$\rho$ 是单同态，G_f可以看成S_n的一个子群。

例：$\rho : G_f \longrightarrow S_{\{\alpha_1,\cdots,\alpha_n\}}$不一定是满同态。$f(x) = (x^2 - 2)(x - 1) \in Q[x]$，$f(x)$在分裂域上有3个根，但$\forall g \in G_f$，一定有$g(1) = 1$，所以$G_f$为$S_3$的真子集。

命题6.5. $f(x)$不可约$\Longleftrightarrow G_f$在$\{\alpha_1,\cdots,\alpha_n\}$上传递。

当$f(x)$不可约时，$[K(\alpha):K]=n$（α为$f(x)$在扩域上的根），而$[K(\alpha):K]$整除$[E:K]$，由引理4.2，$[E:K]=|G_f|$，所以G_f在$\{\alpha_1,\cdots,\alpha_n\}$ 上传递时，$n\mid|G_f|$。

例如$f(x)$为K上的二次多项式，$f(x)$可约时，$G_f\cong\{id\}$，$f(x)$不可约时，$G_f\cong S_2$。

对于K上的多项式$f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$，在分裂域$E$上可以写成$f(x)=\prod\limits_{i=1}^{n}(x-\alpha_i)$。

令

$$\Delta(f)=\prod_{1\le i<j\le n}(\alpha_i-\alpha_j),\quad D(f)=(\Delta(f))^2=\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2$$

因为$f(x)$没有重根，所以$\Delta(f)\neq0$。G_f看成S_n的子群，$\forall g\in G_f$

$$g(\Delta(f))=\prod_{1\le i<j\le n}(g(\alpha_i)-g(\alpha_j))=(-1)^{\tau(g)}\cdot\Delta(f)$$

若g为奇置换，$g(\Delta(f))=-\Delta(f)$，若g 为偶置换，$g(\Delta(f))=\Delta(f)$。

命题6.6. G_f有奇置换$\Longleftrightarrow \Delta(f)\notin K$。

证：" $\Longrightarrow$ " 设$g\in G_f$为奇置换，$g(\Delta(f))\neq\Delta(f)$。而$G_f$中元素是保持$K$中元素不动的自同构，所以$\Delta(f)\notin K$。

" $\Longleftarrow$ " 若$\Delta(f)\notin K$，必存在$g\in G_f$，使得$g(\Delta(f))\neq\Delta(f)$，则$g$为奇置换。

我们发现$D(f)=(\Delta(f))^2=\prod\limits_{1\le i<j\le n}(\alpha_i-\alpha_j)^2$，$\forall g\in G_f$，$g(D(f))=D(f)$，所以$D(f)\in K$。

定义6.7. 设$P(x_1,\cdots,x_n)\in K[x_1,\cdots,x_n]$，若对$\forall\sigma\in S_n$，

$$P(x_1,\cdots,x_n)=P(x_{\sigma(1)},\cdots,x_{\sigma(n)})$$

则称P为**对称多项式**。

令

$$\begin{cases}\sigma_1=x_1+\cdots+x_n\\ \sigma_2=x_1x_2+x_1x_3+\cdots+x_{n-1}x_n\\ \quad\vdots\\ \sigma_n=x_1x_2\cdots x_n\end{cases}$$

σ_i为$x_1,\cdots,x_n$中任意i个元素乘积之和，称$\sigma_1,\cdots,\sigma_n$为$x_1,\cdots,x_n$的基本对称多项式。

P，Q均为多项式，$P(x_1,\cdots,x_n)=Q(\sigma_1,\cdots,\sigma_n)\Longleftrightarrow P$为对称多项式。$D(f)=\prod\limits_{1\le i<j\le n}(\alpha_i-\alpha_j)^2$显然为一个关于$\alpha_1,\cdots,\alpha_n$的对称多项式。

6.1 三次多项式的Galois群

设$f(x)$为K上的三次多项式，在分裂域上有3个根x_1，x_2，x_3，要判断G_f中有没有奇置换，我们就要计算一下$D(f)$。

设$P(x_1,x_2,x_3)=((x_1-x_2)(x_1-x_3)(x_2-x_3))^2$，把等式右边展开之后的项$x_1^ix_2^jx_3^k$记为$(i,j,k)$。我们将展开后的各项按$x_i$的次数从高到低进行排列，设$i\ge j\ge k$，可分为五项，依次为$(4,2,0)$，$(4,1,1)$，$(3,3,0)$，$(3,2,1)$，$(2,2,2)$。因为$P$为对称多项式，$(4,2,0)$这一项代表的是$a_1(x_1^4x_2^2+x_1^4x_3^2+x_2^4x_1^2+x_2^4x_3^2+x_3^4x_1^2+x_3^4x_2^2)$，$(4,1,1)$是指$a_2(x_1^4x_2x_3+x_2^4x_1x_3+x_3^4x_1x_2)$，另外3项同理可得。

基本对称多项式与原多项式的系数有这样的关系，$\sigma_k=(-1)^ka_k$，因此我们想把$P(x_1,\cdots,x_n)$转化为$Q(\sigma_1,\cdots,\sigma_n)$的形式，可以在不求出$x_1,\cdots,x_n$的情况下，仅仅依靠系数就能进行计算。

按照前面对单项式的排列方法，σ_i中的最高项为$x_1x_2\cdots x_i$，则$\sigma_1^{l_1}\sigma_2^{l_2}\cdots\sigma_n^{l_n}$中的最高项为$x_1^{l_1+l_2+\cdots+l_n}x_2^{l_2+\cdots+l_n}\cdots x_n^{l_n}$，所以$x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$与$\sigma_1^{i_1-i_2}\sigma_2^{i_2-i_3}\cdots\sigma_{n-1}^{i_{n-1}-i_n}\sigma_n^{i_n}$的最高项相同。可以用$\sigma_1^{i-j}\sigma_2^{j-k}\sigma_3^k$将$P(x_1,x_2,x_3)$的每一项消掉，最后得到

$$P(x_1,x_2,x_3)=A\sigma_1^2\sigma_2^2+B\sigma_1^3\sigma_3+C\sigma_2^3+D\sigma_1\sigma_2\sigma_3+E\sigma_3^2$$

只要确定了各项系数就可以算出$P(x_1,x_2,x_3)$的值。

给x_1,x_2,x_3赋值，用待定系数法可求出$A=1$，$B=-4$，$C=-4$，$D=18$，$E=-27$，则

$$P(x_1,x_2,x_3)=\sigma_1^2\sigma_2^2-4\sigma_1^3\sigma_3-4\sigma_2^3+18\sigma_1\sigma_2\sigma_3-27\sigma_3^2$$

$D(f)$就可以通过$P(x_1,x_2,x_3)$来求得，然后看$\Delta(f)$是不是属于K。若$\Delta(f)\notin K$，$G_f\cong S_3$，会有下面的表

$$\begin{array}{ccccc} K & \subseteq & M & \subseteq & E \\ \downarrow & & \downarrow & & \downarrow \\ S_3 & \rhd & A_3 & \rhd & \{id\} \end{array}$$

经过计算验证，我们会发现$K(\Delta(f))$对应的Galois群恰好就是A_3，也就是说$M = K(\Delta(f))$，而且$\Delta(f)$在K上的极小多项式为$x^2 - (\Delta(f))^2$。

例：$f(x) = x^3 + x^2 - 2x + 1 \in Q[x]$，在$Q$上不可约。$D(f) = -31$，$\Delta(f) = \pm\sqrt{-31} \notin Q$，所以$G_f$中有奇置换，且$3 \mid |G_f|$，则$G_f \cong S_3$。

例：$f(x) = x^3 - 3x + 1 \in Q[x]$，在$Q$上不可约。$D(f) = 81$，$\Delta(f) = \pm 9 \in Q$，所以$G_f$中没有奇置换，且$3 \mid |G_f|$，则$G_f \cong A_3$。

6.2 四次多项式的Galois群

设$f(x) = x^4 + bx^3 + cx^2 + dx + e$是$K$上的不可约多项式，$f(x)$没有重根，$E$为$f(x)$的分裂域，在$E$上有$f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$，我们先假定$G_f = S_4$。

对于

$$\begin{array}{ccccccc}
K & \subseteq & K(\Delta(f)) & \subseteq & M & \subseteq & E \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
S_4 & \rhd & A_4 & \rhd & K_4 & \rhd & \{id\}
\end{array}$$

我们想求出K_4对应的Galois群M，M中元素是在K_4作用下不动的。

令

$$\begin{cases}
\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4 \\
\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4 \\
\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3
\end{cases}$$

我们发现$\{\beta_1, \beta_2, \beta_3\}$在$K_4$作用下还是$\{\beta_1, \beta_2, \beta_3\}$。$K(\beta_1, \beta_2, \beta_3)$对应的中间群为$Gal(E/K(\beta_1, \beta_2, \beta_3))$，而$Gal(E/K(\beta_1, \beta_2, \beta_3)) = \{\tau \in S_4 \mid \tau(\beta_i) = \beta_i, i = 1, 2, 3\}$，经过计算得到，$Gal(E/K(\beta_1, \beta_2, \beta_3)) = K_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$，也就是说$M = K(\beta_1, \beta_2, \beta_3)$。

容易验证，$\{\beta_1, \beta_2, \beta_3)\}$在$S_4$的作用下是一条轨道。设$g(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3)$，则$g(x)$在$G_f$的作用下是不变的。$G_f$中元素为$K-$同构，所以$g(x) \in K[x]$，且$K(\beta_1, \beta_2, \beta_3)$为$g(x)$的分裂域。

$g(x) = x^3 - (\beta_1 + \beta_2 + \beta_3)x^2 + (\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3)x + \beta_1\beta_2\beta_3$

其中$\beta_1+\beta_2+\beta_3=\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_1\alpha_4+\alpha_2\alpha_3+\alpha_2\alpha_4+\alpha_3\alpha_4=\sigma_2=c$，$\beta_1\beta_2+\beta_1\beta_3+\beta_2\beta_3$是对称的，将$\beta_1,\beta_2,\beta_3$代入后展开，按次数排列有两项$(2,1,1,0)$和$(1,1,1,1)$，则$\beta_1,\beta_2,\beta_3$ 可化为$A\sigma_1\sigma_3+B\sigma_4$，用待定系数法可确定$A=1$，$B=-4$。同样，$\beta_1\beta_2\beta_3$展开后有$(3,1,1,1)$，$(2,2,2,0)$，$(2,2,1,1)$，可表示成$A\sigma_1^2\sigma_4+B\sigma_3^2+C\sigma_2\sigma_4$，用待定系数法求得$A=-1$，$B=-1$，$C=4$，则有

$$\begin{aligned}g(x)=&x^3-\sigma_2x^2+(\sigma_1\sigma_3-4\sigma_4)x-\sigma_1^2\sigma_4-\sigma_3^2+4\sigma_2\sigma_4\\=&x^3-cx^2+(bd-4e)x-b^2e-d^2+4ce\end{aligned}$$

由于$\beta_1-\beta_2=\alpha_1\alpha_2+\alpha_3\alpha_4-\alpha_1\alpha_3-\alpha_2\alpha_4=(\alpha_1-\alpha_4)(\alpha_2-\alpha_3)$，$\beta_1-\beta_3=(\alpha_1-\alpha_3)(\alpha_2-\alpha_4)$，$\beta_2-\beta_3=(\alpha_1-\alpha_2)(\alpha_3-\alpha_4)$

$$\begin{aligned}\Delta(g)=&(\beta_1-\beta_2)(\beta_1-\beta_3)(\beta_2-\beta_3)\\=&(\alpha_1-\alpha_4)(\alpha_2-\alpha_3)(\alpha_1-\alpha_3)(\alpha_2-\alpha_4)(\alpha_1-\alpha_2)(\alpha_3-\alpha_4)\\=&\Delta(f)\end{aligned}$$

因此计算四次多项式的$\Delta(f)$可转化为计算三次多项式的$\Delta(g)$。

前面的过程都在假定$f(x)$的Galois群是S_4的前提下，那么给了一个K上的四次不可约多项式$f(x)$（K的特征为0）。我们来确定它的Galois群。

首先计算$g(x)$。$K(\beta_1,\beta_2,\beta_3)$是$g(x)$的分裂域。$G_g$为$g(x)$的Galois群。然后判断$g(x)$在$K$上是否可约。若$g(x)$不可约，可通过前面计算三次多项式Galois群的方法来计算G_g。若$g(x)$可约，则$g(x)$可写成三个一次因式或一个一次因式和一个二次因式的乘积，G_g的计算就更容易了。

$Gal(E/K(\beta_1,\beta_2,\beta_3))=K_4\cap G_f$，由于$K(\beta_1,\beta_2,\beta_3)$为$g(x)$的分裂域，$K(\beta_1,\beta_2,\beta_3)/K$是Galois扩张，由Galois 基本定理，$G_g\cong G_f/K_4\cap G_f$。

$$\begin{tikzcd}
K \arrow[d] & \subseteq & K(\Delta(f)) \arrow[d] & \subseteq & K(\beta_1,\beta_2,\beta_3) \arrow[d] & \subseteq & E \arrow[d] \\
S_4 \arrow[d] & \rhd & A_4 \arrow[d] & \rhd & K_4 \arrow[d] & \rhd & \{id\} \arrow[d] \\
G_f & \rhd & A_4\cap G_f & \rhd & K_4\cap G_f & \rhd & \{id\}
\end{tikzcd}$$

又因为$4 \mid |G_f|$，所以G_f有以下几种情况

$\lvert G_g\rvert$	$\lvert G_f\rvert$	G_f
6	24	S_4
3	12	A_4
2	8	$D_4 \cong K_4\{(1),(12)\}$
2	4	$C_4 \cong <(1234)>$
1	4	K_4

因此，我们可以通过$g(x)$来计算G_g，然后根据表格来推断出G_f，当$|G_g| = 2$时，$G_f = D_4$或C_4。下面看$f(x)$在$K(\beta_1,\beta_2,\beta_3)$上是否可约，当$f(x)$在$K(\beta_1,\beta_2,\beta_3)$上不可约时，$K(\beta_1,\beta_2,\beta_3)$对应的Galois群在$f(x)$的根的集合$\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$上是传递的，$G_f$只能是$D_4$，若是$C_4$的话，$K_4 \cap C_4$中有两个元素，在$\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$上是不传递的。当$f(x)$在$K(\beta_1,\beta_2,\beta_3)$上可约时，$G_f = C_4$。

例：$f(x) = x^4 - 4x + 2 \in Q[x]$，由Eisenstein判别法可知，$f(x)$在$Q$上不可约。$g(x) = x^3 - 8x + 16$在$Q$上不可约，$(\Delta(f))^2 = (\Delta(g))^2 = -4864$，所以$\Delta(g) \notin Q$，则$G_g = S_3$。查表可得，$G_f = S_4$。

例：$f(x) = x^4 + 4x^2 + 2 \in Q[x]$，由Eisenstein判别法可知，$f(x)$在$Q$上不可约。$g(x) = (x-4)(x^2-8)$，分裂域为$M = Q(\sqrt{2})$，$|G_g| = 2$，而$f(x)$在$Q(\sqrt{2})$上可约，所以$G_f = C_4$。

例：$f(x) = x^4 - 10x^2 + 4 \in Q[x]$，因为在$Q$上没有根，$f(x)$在$Q$上不可约。$g(x) = (x+10)(x+4)(x-4)$，$|G_g| = 1$。查表可得，$G_f = K_4$。

7 分圆扩张与循环扩张

7.1 分圆扩张

设K是一个域，$charK = 0$，$f(x) = x^n - 1 \in K[x]$在其分裂域E上有n个根1，ξ_1，ξ_2，$\cdots$，ξ_{n-1}，这n个根构成一个循环群$< \xi_1 >$，$\xi_i = \xi_1^i$，且$|\xi_1| = n$，我们称ξ_1为n次本原单位根。当$(i,n) = 1$时，ξ_1^i也是一个n次本原单位根。那么$E = K(1, \xi_1, \cdots, \xi_{n-1}) = K(\xi)$（$\xi$为一个$n$次本原单位根）。$E$为分裂域，所以$E/K$为Galois扩张。

设$G_f = Gal(E/K)$，$\forall g \in G_f$，存在i，$(i,n) = 1$，使$g(\xi) = \xi^i$，则存在一个群同态$\sigma : G_f \longrightarrow (Z/(n))^*$，使$\sigma(g) = \bar{i}$。而$g$由$i$唯一确定，所以$\sigma$为单同态，特别的，当$K = Q$时，$G_f \cong (Z/(n))^*$。

注7.1. $(Z/(n))^*$在乘法意义下构成一个群。当$n = 2$时，$(Z/(2))^* = \{\bar{1}\}$；当$n = 6$时，$(Z/(6))^* = \{\bar{1}, \bar{5}\}$是一个2阶循环群；当$n = 12$时，$(Z/(12))^* = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\} \cong K_4$。$(Z/(n))^*$是一个$\varphi(n)$阶的交换群，若$n = p_1^{r_1} \cdots p_s^{r_s}$，$(Z/(n))^* \cong (Z/(p_1^{r_1}))^* \times \cdots \times (Z/(p_s^{r_s}))^*$。

设ξ是一个n次本原单位根，则全部的n次本原单位根为ξ^i，其中$(i,n) = 1$，$1 \le i \le n-1$，记

$$\Phi_n(x) = \prod_{(i,n)=1, 1 \le i \le n-1} (x - \xi^i)$$

当K的特征为0时（即$K = Q$），称$\Phi_n(x)$为分圆多项式，其次数为欧拉函数$\varphi(n)$。而且我们有

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

例：$\Phi_1(x) = x - 1$，$\Phi_2(x) = x + 1$，$\Phi_3(x) = x^2 + x + 1$

$\Phi_4(x) = \frac{x^4-1}{(x-1)(x+1)} = x^2 + 1$，$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$

$\Phi_6(x) = \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1$

当p为素数时，$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$

因为$x^n - 1$为首1的整系数多项式，则它所有首1的有理因式也是整系数多项式，故分圆多项式$\Phi_n(x)$为首1的整系数多项式。

命题7.2. $\Phi_n(x)$是Q上的不可约多项式。

$\Phi_n(x)$在Q上不可约需要在模p的域上说明，在此不给出证明。

由上述命题可知，$f(x)$的n次本原单位根在Q上的极小多项式为$\Phi_n(x)$。$|G_f| = deg\Phi_n(x) = \varphi(n)$，所以$G_f \cong (Z/(n))^*$。

7.2 循环扩张

在对$f(x) = x^n - 1$的Galois群有所了解之后，我们来看一下$f(x) = x^n - c$的Galois群。设$f(x)$为K上的不可约多项式。

若K包含x^n-1的所有根，则$f(x)$的分裂域$E = K(\alpha, \alpha\xi, \cdots, \alpha\xi^{n-1}) = K(\alpha)$，若$K$不包含$x^n - 1$的所有根，设$M = K(\xi)$，则$E = M(\alpha)$。

命题7.3. 设K包含$x^n - 1$的所有根，$f(x) = x^n - c \in K[x]$，则G_f是循环群。

证：设E是$f(x)$在K上的分裂域，α为$f(x)$的一个根，则$f(x)$所有根为α，$\alpha\xi$，$\cdots$，$\alpha\xi^{n-1}$（ξ为n次本原单位根），$E = K(\alpha)$。对于$\forall g \in G_f$，存在