定義 8 ax^3+bx^2+cx+d を複素数係数の 3 次式で重根をもたないものとする．

1. $\{(x,y)\in\mathbb{C}^2 \mid y^2=ax^3+bx^2+cx+d\}$ に無限遠点 O を付け加えたもの E を楕円曲線という．

2. $\mathbb{C}(E)=\mathbb{C}(x,y)=\{f+gy \mid f,g$ は複素数係数の x の有理式 $\}$ を E の関数体という．$\mathbb{C}(E)$ の乗法は $(f+gy)(h+ky)=fh+gk(ax^3+bx^2+cx+d)+(fk+gh)y$ で定める．

3. E の点の整数係数の形式的な線形結合 $D=n_1[P_1]+\cdots+n_k[P_k]$ を E の因子という．因子 D の係数の和 $n_1+\cdots+n_k$ を D の次数といい $\deg D$ で表す．

E の因子全体のなす加法群を E の因子群といい $\mathrm{Div}(E)$ で表す．$\mathrm{Div}(E)$ の部分群 $\{D\in \mathrm{Div}(E) \mid \deg D=0\}$ を $\mathrm{Div}^0(E)$ で表す．

4. E の有理関数 $f\in\mathbb{C}(E), f\neq 0$ に対し，$\sum_{P:f(P)=0}\mathrm{ord}_P f\cdot[P]+\sum_{P:f(P)=\infty}\mathrm{ord}_P f\cdot[P]$ を f の因子といい $\mathrm{div}\ f$ で表す．

5. $\dfrac{dx}{y}$ の定数倍を E 上の正則微分形式という．

定理 9 (Abel-Jacobi の定理) E を楕円曲線とする．

1. E の有理関数 f の因子の次数 $\deg\mathrm{div}\ f$ は 0 である．

2. E の因子 D の次数が 0 ならば，$D=[P]-[O]+\mathrm{div}\ f$ をみたす有理関数 f が存在するような E の点 P がただ 1 つ存在する．

定義 10 集合 A と加法 $+\colon A\times A\to A$ が次の条件 (1)–(4) をすべてみたすとき，A は（$+$ に関して）可換群であるという．

(1) A の任意の元 a,b,c に対し $(a+b)+c=a+(b+c)$ がなりたつ．

(2) A の元 0 で，A の任意の元 a,b,c に対し $a+0=a$ をみたすものがただ 1 つ存在する．

(3) 0 を (2) の条件をみたす A の元とする．A の任意の元 a に対し $a+b=0$ をみたす A の元 b がただ 1 つ存在する．

(4) A の任意の元 a,b に対し $a+b=b+a$ がなりたつ．

(2) の元 0 を A の零元といい，(3) の元 b を a の逆元という．

定義 11 A と A' を可換群とする．

1. 写像 $f\colon A\to A'$ が次の条件 (1) をみたすとき，f は可換群の射であるという．可換群の準同形であるともいう

(1) A の任意の元 a,b に対し $f(a+b)=f(a)+f(b)$ である．

2. $f\colon A\to A'$ を可換群の射とする．A の部分群 $\{a\in A \mid f(a)=0\}$ を f の核といい $\mathrm{Ker}(f\colon A\to A')$ で表す．A' の商群 $A'/f(A)$ を f の余核といい $\mathrm{Coker}(f\colon A\to A')$ で表す．

$\mathrm{Div}^0(E)$ は可換群の射 $\deg\colon \mathrm{Div}(E)\to\mathbb{Z}$ の核である．可換群の射 $\mathrm{div}\colon \mathbb{C}(E)^\times\to\mathrm{Div}^0(E)$ の余核を次数 0 の因子類群とよび，$\mathrm{Pic}^0(E)$ で表す．

定理 12 (Abel-Jacobi の定理のいいかえ) E の点 P を因子類 $\overline{[P]-[O]}$ にうつす写像 $E\to\mathrm{Pic}^0(E)$ は全単射である．

定理 13 E を楕円曲線とし，ω を E 上の正則微分形式とする．

1. 位相群の射 $p\colon\mathbb{C}\to E$ で，E の原点 O のまわりで $p(\int_O^P\omega)=P$ をみたすものがただ 1 つ存在する．

2. $\mathbb{C}$ の $\mathbb{R}$ 上の基底 ω_1,ω_2 で $\{z\in\mathbb{C}\mid p(z)=0\}=\{n\omega_1+m\omega_2 \mid n,m\in\mathbb{Z}\}$ をみたすものが存在する．