1　平面3次曲線

1.1　結合律のための準備

平面3次曲線の点にアーベル群の構造が入ることを示す中で、特に結合律が成り立つことは自明でない。その証明のために準備する。

補題 1.1. 相異なる5点 $P_1, \ldots, P_5 \in \mathbb{P}^2$ が、どの4点も一直線上にないならば、その5点を通る2次曲線は高々1つ。

(証明). 相異なる2次曲線 C, C' で $P_1, \ldots, P_5$ を通るものがあると仮定する。このとき $F, F' \in \Lambda_2(\{P_1, \ldots, P_5\})$ によって $C = \mathcal{Z}(F), C' = \mathcal{Z}(F')$ と表せる。$C \cap C' \supset \{P_1, \ldots, P_5\}$ が成り立つから弱ベズーの定理より、F, F' は共通因子を持つ。$C \neq C'$ から、共通因子は1次式。

$F = GH, F' = GH'$ が成り立つように $G, H, H' \in \Lambda_1$ を取る。$L := \mathcal{Z}(G), M := \mathcal{Z}(H), M' := \mathcal{Z}(H')$ とおくと、$C \neq C'$ より $M \neq M'$。

$$C = L \cup M, C' = L \cup M'$$

となるから、

$$\begin{aligned} C \cap C' &= (L \cup M) \cap (L \cup M') \\ &= L \cup (M \cap M') \\ &\in \{P_1, \ldots, P_5\} \end{aligned}$$

M, M' は直線で $M \neq M'$ だから $M \cap M'$ は高々1点。よって直線 L 上に4点があり、仮定に矛盾する。 ∎

さらに、定理の証明には以下が必要である。証明はこの二つの補題の証明は演習問題。

補題 1.2. k を代数的閉体だとする。$F \in k[X, Y, Z] \setminus \{0\}$ によって $C := \mathcal{Z}(F)$ とおくと、

$$|C| = \infty$$

補題 1.3. k を無限体とする。$L \subset \mathbb{P}^2$ が直線なら、

$$|L| = \infty$$

こちらは証明が難しい。

命題 1.4. k を無限体とする。$F \in \Lambda_2[X, Y, Z], C := \mathcal{Z}(F)$ とおく。このとき、

$$|C| \neq 0 \implies |C| = \infty$$

定理 1.5. k を無限体とする。相異なる8点 $P_1, \ldots, P_8 \in \mathbb{P}^2_k$ はどの4点も一直線上に無く、どの7点も既約2次曲線上に無いとする。この時、

$$\dim \Lambda_3(\{P_1, \ldots, P_8\}) = 2$$

となる。

(証明). 前章の補題から

$$\dim \Lambda_3(\{P_1, \ldots, P_8\}) \geq 10 - 8 = 2$$

が分かる。以下では $\leq$ も成り立つことを示す。そのために与えられた 8 点の分布の仕方によって場合分けをする。

場合 I

8 点 $P_1, \ldots, P_8$ が以下を満たす場合。

1. どの 3 点も 1 つの直線上にない
2. どの 6 点も 1 つの 2 次曲線上にない

もしある 6 点が可約な 1 つの 2 次曲線上にあるとすると、それらの点は 2 本の直線に載っている。したがって条件 2. と条件 1. とを満たす 8 点は「どの 6 点も 1 つの既約 2 次曲線上にない」も満たす。

$\dim \Lambda_3(\{P_1, \ldots, P_8\}) \geq 3$ として矛盾を導く。直線 L を 2 点 P_1, P_2 を結ぶものとする（L の定義式も L と表す)。このとき条件 1. より $P_1, \ldots, P_8 \notin L$ となる。互いに異なる 2 点 P_9, P_{10} を $L \setminus \{P_1, P_2\}$ から取る。前章の補題より、

$$\dim \Lambda_3(\{P_1, \ldots, P_8\} \cup \{P_9, P_{10}\}) \geq 3 - 2 = 1$$

となるので、$F \in \Lambda_3(\{P_1, \ldots, P_{10}\}) \setminus \{0\}$ が取れる。

曲線 $C := \mathcal{Z}(F)$ を考える。$C \cap L \subset \{P_1, P_2, P_9, P_{10}\}$ となるから、

$$|C \cap L| \geq 4 > \deg C \cdot \deg L = 3$$

したがって弱ベズーの定理より、F と L は共通因子を持つ。L は既約なので、ある $G \in \Lambda_2$ が存在して $F = L \cdot G$ となる。さらに $P_3, \ldots, P_8 \notin L$ から $P_3, \ldots, P_8 \notin \mathcal{Z}(G)$ が分かる。これは条件 2. に反する。

条件 1., 2. と $\dim \Lambda_3(\{P_1, \ldots, P_8\}) \geq 3$ を仮定して条件 2. と矛盾したが、条件 1., 2. を満たす点の分布は存在する。よって $\dim \Lambda_3(\{P_1, \ldots, P_8\}) \geq 3$ は否定され、

$$\text{条件 1., 2.} \implies \dim \Lambda_3(\{P_1, \ldots, P_8\}) = 2$$

が成立する。

場合 II

3 点 $P_1, \ldots, P_3$ が直線 L 上にある場合。

$P_9 \in L \setminus \{P_1, P_2, P_3\}$ を取る。前章の補題より、

$$\dim \Lambda_3(\{P_1, \ldots, P_8, P_9\}) \geq 10 - 9 = 1$$

となるので、$F \in \Lambda_3(\{P_1, \ldots, P_9\}) \setminus \{0\}$ が取れる。そして場合 I と同様に $G \in \Lambda_2$ が存在して $F = L \cdot G$ となる。ここで定義の前提より $P_4, \ldots, P_8 \notin L$ であった。したがって $P_4, \ldots, P_8 \in \mathcal{Z}(G)$。つまり

$$G \in \Lambda_3(\{P_4, \ldots, P_8\})$$

F は $\Lambda_3(\{P_1,\dots,P_9\})\setminus\{0\}$ から任意に取り、また $\{P_1,P_2,P_3,P_9\}\subset L$ だから

$$\Lambda_3(\{P_1,\dots,P_9\})=L\cdot\Lambda_3(\{P_4,\dots,P_8\})\subset\Lambda_3$$

補題 1.1 より $\dim\Lambda_3(\{P_4,\dots,P_8\})=1$。ゆえに

$$\Lambda_3(\{P_1,\dots,P_9\})=1$$

よって

$$\dim\Lambda_3(\{P_1,\dots,P_8\})\leq 2$$

場合 III

6 点 $P_1,\dots,P_6$ が既約 2 次曲線 $D:=\mathcal{Z}(G)$ 上にある場合。

$P_9\in D\setminus\{P_1,\dots,P_6\}$ を取る。前章の補題より、

$$\dim\Lambda_3(\{P_1,\dots,P_8,P_9\})\geq 10-9=1$$

となるので、$F\in\Lambda_3(\{P_1,\dots,P_9\})\setminus\{0\}$ が取れる。そして場合 I と同様に $L\in\Lambda_1$ が存在して $F=L\cdot G$ となる。ここで定義の前提より $P_7,P_8\notin D$ であった。したがって $P_7,P_8\in L$。つまり

$$L\in\Lambda_1(\{P_7,P_8\})$$

F は $\Lambda_3(\{P_1,\dots,P_9\})\setminus\{0\}$ から任意に取り、また $\{P_1,P_2,P_3,P_9\}\subset L$ だから

$$\Lambda_3(\{P_1,\dots,P_9\})=G\cdot\Lambda_3(\{P_7,P_8\})\subset\Lambda_3$$

$\dim\Lambda_1(\{P_7,P_8\})=1$ であるから、

$$\Lambda_3(\{P_1,\dots,P_9\})=1$$

よって

$$\dim\Lambda_3(\{P_1,\dots,P_8\})\leq 2$$

∎

系 1.6. k を無限体とする。$C_1,C_2\subset\mathbb{P}^2$ を共通成分を持たない 3 次曲線とし、

$$C_1\cap C_2=\{P_1,\dots,P_9\}$$

とおく。この時、任意の 3 次曲線 $C\subset\mathbb{P}^2$ について

$$P_1,\dots,P_8\in C\implies P_9\in C$$

が成り立つ。

(証明). $\{P_1,\dots,P_8\}$ はどの 4 点も一直線上に無い。実際、ある 4 点は直線 L 上に会ったとすると、$|C_i\cap L|\geq 4>3\cdot 1=3(i=1,2)$ となり、弱ベズーの定理から $L\subset C_i$。よって $L\subset(C_1\cap C_2)$ となり、C_1 と C_2 が共通因子を持たないことに反

する。同様にして、どの 7 点も 1 つの既約 2 次曲線上に無い。ゆえに $\{P_1, \ldots, P_8\}$ は定理の仮定を満たす。したがって $\dim \Lambda_3(\{P_1, \ldots, P_8\}) = 2$。

$C_i = \mathcal{Z}(F_i)$ とすると、$C_1 \neq C_2$ より、F_1, F_2 は一次独立である。さらに

$$F_1, F_2 \in \Lambda_3(\{P_1, \ldots, P_8\}), \dim \Lambda_3(\{P_1, \ldots, P_8\}) = 2$$

であるから、F_1, F_2 は $\Lambda_3(\{P_1, \ldots, P_8\})$ の基底となっている。よってある斉次多項式 $F \in \Lambda_3(\{P_1, \ldots, P_8\})$ によって 3 次曲線 $C = \mathcal{Z}(F)$ と置くと、

$$F = aF_1 + bF_2 (a, b \in k)$$

の様になる。このことから直ちに

$$C \supset C_1 \cap C_2$$

が分かる。 ∎

1.2 平面 3 次曲線にはアーベル群の構造が入る

定義 1.7. 3 次斉次多項式 $F \in k[X, Y, Z] \setminus \{0\}$ によって $C := \mathcal{Z}(F)$ とおく。この C に対し、以下のように二項演算 $* : C \times C \to C$ を定める。2 点 $P, Q \in C$ を取る。

- $P \neq Q$ の時
  - $\#(\overline{PQ} \cap C) = 3$ の時、$P * Q = (\overline{PQ} \cap C) \setminus \{P, Q\}$
  - $\#(\overline{PQ} \cap C) = 2$ の時、
    - $\overline{PQ}$ が P に於いて C に接する時、$P * Q = P$
    - $\overline{PQ}$ が Q に於いて C に接する時、$P * Q = Q$
- $P = Q$ の時、L を P に於ける C の接線として、
  - $\#(L \cap C) = 2$ の時、$P * Q = (L \cap C) \setminus \{P\}$
  - $\#(L \cap C) = 1$ の時、$P * Q = P$

場合分けが上の定義で尽くされることと $P * Q$ が存在することはベズーの定理による。

注意 1.8. 定義から明らかに $P*Q = Q*P$。更に $R = P*Q$ の時、$P*R = R*Q = Q$ が成立する。$Q * R$ でも同様。

さて、点 $O \in C$ を 1 つ取って固定する。その上で二項演算 $+$ を以下のように定める。

$$\begin{array}{rcl} + : C \times C & \to & C \\ (P, Q) & \mapsto & (P * Q) * O \end{array}$$

これがアーベル群を作る。

定理 1.9. $(C,+)$ はアーベル群を成す。

(証明). 以下を順に示す。ただし $P,Q,R\in C$ とする。

1. $P+Q=Q+P$(可換律の成立)
2. O が単位元 (単位元の存在)
3. P の逆元は $P*(O*O)$(逆元の存在)
4. $(P+Q)+R=P+(Q+R)$(結合律の成立)

(1.) 注意 1.8 より、

$$P+Q=(P*Q)*O=(Q*P)*O=Q+P$$

(2.) $R:=P*O$ と置くと、注意 1.8 より $R*O=P$。よって

$$P+O=(P*O)*O=R*O=P$$

(3.) $O:=O*O$ とおく。さらに $Q:=P*O'=P*(O*O)$ とすれば、

$$P*Q=O',O'*O=O$$

ゆえに

$$P+Q=(P*Q)*O=O'*O=O$$

すなわち $-P=Q=P*(O*O)$。

(4.) まず $P\neq Q$ として証明する。

$$\begin{aligned}(P+Q)+R &= (((P*Q)*O)*R)*O\\ P+(Q+R) &= (P*((Q*R)*O))*O\end{aligned}$$

なので示したいことは $(P+Q)*R=P*(Q+R)$ と同値。

直線 L_1,L_2,L_3 と M_1,M_2,M_3 を以下のように定義する。

$$\begin{aligned}&L_1=\overline{P,Q},\ L_2=\overline{Q+R,O},\ L_3=\overline{P+Q,R}\\ &M_1=\overline{Q,R},\ M_2=\overline{O,P+Q},\ M_3=\overline{P,Q+R}\end{aligned}$$

そしてこれらを用いて 3 次曲線 L,M を

$$L:=L_1\cup L_2\cup L_3,M:=M_1\cup M_2\cup M_3$$

定義し、これらの交点を考える。

$$\begin{aligned}\mathcal{J} &:= \{P,Q,R,O,P*Q,Q*R,P+Q,Q+R\}\\ T &:= L_3\cap M_3\end{aligned}$$

と定義すると明らかに $L\cap M=\mathcal{J}\cup\{T\}$ である。この時、$J\subset C$ なので、系 1.6 より $T\in C$ が成り立つ。ここで $C\cap L=\{(P+Q)*R\}\cup\mathcal{J}$ であるから、$T=(P+Q)*R$。同様に $C\cap M$ を考えて、$T=P*(Q+R)$。

次に $P = Q$ として証明する。これは二項演算子 + の連続性を用い、$P \to Q$ の極限として結合律を証明する。まず写像 $\phi_1, \phi_2 : C^3 \to C$ を以下で定義する。

$$\phi_1(P,Q,R) = (P+Q)+R \tag{1}$$
$$\phi_2(P,Q,R) = P+(Q+R) \tag{2}$$

さらに

$$E = \{(P,Q,R) \in C^3 : \phi_1(P,Q,R) = \phi_2(P,Q,R)\}$$

これは Zariski 位相で閉。示したいことは $E = C^3$ と表現できる。一方、

$$\sqcup = \{(P,Q,R) \in C^3 : \#(\mathcal{J} \cup \{T\}) = 9\}$$

（ただし $\mathcal{J}$ は上で定めたもの）とおくと、$\sqcup$ は C^3 の空ではない開集合となる。C^3(既約) の中で $\sqcup$ が稠密であることは前半の証明から分かる。

$$\sqcup \subset E \subset C^3$$

なので、閉包 $\bar{\sqcup}$ が $\sqcup$ を含む最小の閉集合であることより、

$$C^3 = \bar{\sqcup} \subset E \subset C^3$$

すなわち $C^3 = E$。 ∎

例 1.10. $y^2 + y = x^3 - x \in \mathbb{A}^2$ を考え、

$$F(X,Y,Z) = Y^2Z + YZ^2 - X^3 + XZ^2$$

として $C := \mathcal{Z}(F)$ を調べる。

補題 1.11. 体 k に於いて $C \subset \mathbb{P}^2$ が特異点を持つ $\iff p := \mathrm{char}(k) = 37$

(証明). $P \in C$ が特異点である必要十分条件は $F_X(P) = F_Y(P) = F_Z(P) = 0$ である。

$$\begin{aligned} F_X &= -3X^2 + Z^2 \\ F_Y &= 2YZ + Z^2 \\ F_Z &= Y^2 + 2YZ + 2XZ \end{aligned}$$

$P = (a:b:c) \in C$ が特異点だとする。$p = 37$ である時に $P = (5:18:1), (32:18:1)$ が特異点であることを示す。 ∎

$O = (0:1:0) \in C$ として群構造を調べる。

補題 1.12. $O * O = O$ が成り立つ。特に任意の $Q \in C$ に対し $-Q = Q * O, Q = (-Q) * O$ が成立し、さらに $P * Q = -(P+Q)$。

(証明). 点 O における C の接線は $Z=0$ であり、これを満たす C 上の点は O しかない。したがって $O*O=O$ が成り立つ。任意の楕円曲線と $Z=0$ と $O=(0:1:0)$ の交点は O だけであり、しかも O における接線は必ず $Z=0$ となるから、これは任意の楕円曲線で成り立つ。

また、$R:=Q*O$ とおくと

$$
\begin{aligned}
& R = Q*O \\
\Longleftrightarrow\ & Q*R = O \\
\Longleftrightarrow\ & (Q*R)*O = O*O \\
\Longleftrightarrow\ & Q+R = O \\
\Longleftrightarrow\ & R = -Q = Q*O
\end{aligned}
$$

となる。このことから更に $(P*Q)*O = P+Q = -(P*Q)$ が分かる。 ∎

補題 1.13. $Q=(a:b:1)$ に対して $-Q=Q*O=(a:-b-1:1)$