ホモロジー代数入門と Weil ペアリングの定義

光成滋生（@herumi）
TEX by 緑川志穂（@elliptic_shiho）

目次

1　はじめに

Pairing 2010 で Silverman[*1]の招待講演がありました．そこでは暗号の本に載ってるのと違った, より抽象的な定義の説明がありました．このテキスト[*2]は多少（どころではない分量になってしまったけど）補足説明してみます．

群, 環, 準同型定理, 位相空間, 多様体のおさらいは駆け足でしますが, 別途勉強しておいたほうがよいでしょう．前半の一部はホモロジー代数入門にもなっています．

1.1　基底

まずはいくつかの基本的な用語から．

R を可換環, M を R 加群とします．可換環は四則演算のうち割り算を考えない集合です．$\mathbb{Z}/m\mathbb{Z} = \{0, \ldots, m-1\}$ とか行列の集合とかそんなのです．R 加群はそれ自体がアーベル群であり, かつ R と掛け算ができるものと思ってよいです．まあ普通成り立ってて欲しいと思う性質が成り立ってます．

つまり $r, r' \in R$, $m, m' \in M$ について

$$
\begin{aligned}
&r(m+m') = rm + rm', \\
&(r+r')m = rm + r'm, \\
&(rr')m = r(r'm), \\
&1 \cdot m = m.
\end{aligned}
$$

可換環 R はそれ自体が R 加群です．また R が体だったら R 加群は R ベクトル空間になります．ベクトル空間だったら基底があります．同様に R 加群 M も, その任意の元を有限個の基底で表せるときがあります．すなわち

[*1] http://www.thlab.net/pairing2010/invited.html#silverman
[*2] このテキストは http://homepage1.nifty.com/herumi/crypt/pairing-def.html を元に緑川さんが TeX に書き起こされました．

有限生成

ある $e_1, \ldots, e_d \in M$ が存在し, 任意の $m \in M$ について $m = \sum_{i=1}^{d} r_i e_i$ となる $r_1, \ldots, r_d \in R$ が存在する.

一次独立

ある $r_1, \ldots, r_d \in R$ について $\sum_{i=1}^{d} r_i e_i = 0$ ならば $r_1 = \cdots = r_d = 0$.

$e_1, \ldots, e_d \in M$ が有限生成と一次独立の両方を満たすとき, それらを基底といいます.

1.2 素朴なペアリング

ペアリングの性質をおさらいします.

$e : M \times M \to R$ で R 双線形なものをペアリングということにします. 片側を固定すると線形写像ということです.

つまり

$$\begin{aligned} e(m + m', m'') &= e(m, m'') + e(m', m''), \\ e(m, m' + m'') &= e(m, m') + e(m, m''), \\ e(am, m') &= ae(m, m'), \\ e(m, am') &= ae(m, m'). \end{aligned}$$

さて暗号でよく使われるペアリングでは, M は 2 個の基底からなる R 加群です. 基底を e_1, e_2 とすると M の元 x, y は $x = ae_1 + be_2$, $y = ce_1 + de_2$ と書けるので, 線形性から

$$e(x, y) = ace(e_1, e_1) + ade(e_1, e_2) + bce(e_2, e_1) + bde(e_2, e_2)$$

となります.

$e_{ij} = e(e_i, e_j)$ とすると

$$e(x, y) = ace_{11} + ade_{12} + bce_{21} + bde_{22}. \tag{1}$$

とくに歪対称 $e(x, y) = -e(y, x)$ が成り立つなら $e_{11} = e_{22} = 0$, $e_{12} = e_{21}$ なので

$$e(x, y) = (ac - bd)e_{12}.$$

これは M の基底 e_1, e_2 と適当な R の元 e_{ij} を決めると式 1 でペアリングを定義してもよいということです. となると単なる線形和ですね.

ただ, これでは暗号には使えません. なぜなら基底 e_1 と $x = ae_1$ が与えられたとき, a を求めることは離散対数問題の困難性から無理だからです. 式 1 を明示的に計算できるならそもそも暗号に使えないということになります.

R を体として, e_i の生成する部分加群を $\langle e_i \rangle := \{ re_i \mid r \in R \}$ とします. M は $\langle e_1 \rangle$ と $\langle e_2 \rangle$ の直和なので, 任意の $x \in M$ にたいして係数は求められなくてもせめて $x = u + v, u \in \langle e_1 \rangle, v \in \langle e_2 \rangle$ と分解できれば何か情報を取れるかもと思ったことがありました. 残念ながら, 実はそういうふうに x を部分群の要素に分解できるなら DH 問題が解けてしまうので分解は無理ということがわかりました. 証明はたいして難しくありません. この定式化をベクトル分解問題とよびました（最初は 2002 年の ISEC, SCIS2003 で吉田さんと発表 cf.

The Vector Decomposition Problem[*3]．その後 Duursma[*4]や, Galbraith [*5]たちが精密化したり, 初期の Homomorphic Encryption[*6]で参照されたりしたようです.

横道にそれましたが, 要は式 1 を違う形で（基底を使わない形で）定式化したいということです. Silverman による解説はそれが主題です.

2 ホモロジー代数

しばらく無味乾燥なホモロジー代数の初歩に入ります. ここは難しくないのですが一度は一歩一歩自分で手を動かして示さないといけないと思います.

キーワードは 「短い完全列があれば長い完全列を作れる」です.

2.1 準同型写像の集合

M, N, P, Q を R 加群とします.

$$\mathrm{Hom}_R(M,N) := \{\, f : M \to N \mid f \text{ は } R \text{ 加群として準同型写像} \,\}$$

とします（以降 $\mathrm{Hom}(M,N)$ と略記）. R 加群として準同型というのは任意の a, $b \in R$, m, $m' \in M$ に対して $f(am+bm') = af(m)+bf(m')$ が成り立つということです.

この $\mathrm{Hom}(M,N)$ は写像の集合なわけですが, これ自体が R 加群になります. 単位元は任意の $m \in M$ について $f(m) = 0$ とする 0 写像です. f について逆元は $(-f)(m) := -f(m)$ で定義します. つまり $f, g \in \mathrm{Hom}(M,N)$ にたいして和を $(f+g)(m) := f(m)+g(m)$, R 倍を $(rf)(m) := r \times f(m)$ で定義するのです.

初めての人は, ここでまず何を示すべきかわかるでしょうか. まず上で定義した和やマイナスや R 倍が正しい定義であること (well-defined) の確認です. それは $f+g \in \mathrm{Hom}(M,N)$ を示すということです. 「一見あたり前」に見えますが,「関数の和が M から N への R 加群としての準同型写像であること」は自明ではありません. それをチェックしてみます.

$$\begin{aligned}(-f)(m+m') &= -f(m+m') && (-f \text{ の定義から})\\ &= -f(m)-f(m') && (f \text{ が準同型だから})\\ &= (-f)(m)+(-f)(m') && (-f \text{ の定義を再び適用}).\end{aligned}$$

$$\begin{aligned}(f+g)(m+m') &= f(m+m')+g(m+m') && (f+g \text{ の定義から})\\ &= f(m)+f(m')+g(m)+g(m') && (f,g \text{ が準同型だから})\\ &= (f+g)(m)+(f+g)(m') && (f+g \text{ の定義を再び適用}).\end{aligned}$$

同様に $(f+g)(am) = a(f+g)(m)$ も示してください. これにより $f+g \in \mathrm{Hom}(M,N)$ を確認できました. $rf \in \mathrm{Hom}(M,N)$ についても, rf という関数の線形性を示す必要があります（自分でやること）.

さて, これで何を示せたのかというと「$\mathrm{Hom}(M,N)$ が R 加群になる」ということです.

[*3] http://search.ieice.org/bin/summary.php?id=e93-a_1_188

[*4] http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.73.8064

[*5] http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.150.53

[*6] http://portal.acm.org/citation.cfm?id=1431888

2.2 Hom から Hom への写像

P, Q, N が R 加群だとすると $\mathrm{Hom}(P,Q)$, $\mathrm{Hom}(N,Q)$ という R 加群を作れました. この Hom から Hom への写像を考えてみます.

$\varphi : N \to P$ という準同型写像があったとしましょう. すると $f \in \mathrm{Hom}(P,Q)$ は P から Q への写像なので φ と合成すると $f \circ \varphi$ は N から Q への写像になります.

$$\overbrace{N \underset{\varphi}{\to} P \underset{f}{\to} Q}^{f \circ \varphi}$$

正確には $(f \circ \varphi)(n) := f(\varphi(n))$ で定義します. $f \circ \varphi \in \mathrm{Hom}(N,Q)$ を確認しましょう.

$$\begin{aligned} f \circ \varphi(an + bn') &= f(\varphi(an + bn')) \\ &= f(a\varphi(n) + b\varphi(n')) \\ &= af(\varphi(n)) + bf(\varphi(n')) \\ &= a(f \circ \varphi)(n) + b(f \circ \varphi)(n') \end{aligned}$$

$f \circ \varphi$ を $\varphi^* f$ とかくことにします. すると φ^* は $f \in \mathrm{Hom}(P,Q)$ を $f \circ \varphi \in \mathrm{Hom}(N,Q)$ に移す写像と考えられます. 実は φ^* は $\mathrm{Hom}(P,Q)$ から $\mathrm{Hom}(N,Q)$ への R 加群として準同型写像になります.

$$\varphi^* : \mathrm{Hom}(P,Q) \to \mathrm{Hom}(N,Q)$$

最初は混乱するかもしれませんが, 大丈夫でしょうか. φ^* が準同型写像だということは $\varphi^*(af + bf') = a\varphi^*(f) + b\varphi^*(f')$ を示す必要があるということです.

くどいですがやってみましょう. 上記の等号を示すということは関数として同じだということを示すことなので

$$\begin{aligned} \varphi^*(af + bf')(n) &= (af + bf')(\varphi(n)) \\ &= af(\varphi(n)) + bf'(\varphi(n)) \\ &= a(\varphi^* f)(n) + b(\varphi^* f')(n) \\ &= (a\varphi^*(f) + b\varphi^*(f'))(n). \end{aligned}$$

一つ目の等号は φ^* の定義, 二つ目の等号は Hom() の演算（和とスカラー倍）の定義, ... となっています.

ここまでの流れをまとめます. P, Q, N が R 加群で準同型 $\varphi : N \to P$ があると準同型写像 $\varphi^* : \mathrm{Hom}(P,Q) \to \mathrm{Hom}(N,Q)$ を構成できる.

2.3 kernel と image

まず単射と全射の復習をしましょう.

単射 $f : P \to Q$ が単射であるとは, $p \in P$ が $f(p) = 0$ である必要十分条件が $p = 0$.
全射 $f : P \to Q$ が全射であるとは, 任意の $q \in Q$ にたいしてある $p \in P$ が存在して $f(p) = q$.

単射は同じものにいくことはない, 全射は全てに行き渡る, というイメージです.

準同型写像 $f : P \to Q$ にたいして

kernel $\mathrm{Ker}(f) := \{\, p \in P \mid f(p) = 0 \,\}$.
image $\mathrm{Im}(f) := \{\, f(p) \mid p \in P \,\}$.

と定義します.

$\mathrm{Ker}(f)$ は f が 0 になる（つぶれてしまう）ような P の元全体, $\mathrm{Im}(f)$ は f の行き先全体ということです. それぞれ f の kernel, image と呼びます.

$\mathrm{Ker}, \mathrm{Im}$ を使って全射と単射を表現すると

- f が単射 $\Leftrightarrow \mathrm{Ker}(f) = \{\, 0 \,\}$
- f が全射 $\Leftrightarrow \mathrm{Im}(f) = Q$

となります. r が単射かつ全射であるとき全単射といい, そのとき P と Q は同型であるといいます.

2.4 部分加群と商加群

P を R 加群とします. P の部分集合 S が

$$s_1 + s_2 \in S \text{ for } s_1, s_2 \in S,$$
$$rs \in S \text{ for } r \in R, s \in S$$

をみたすとき S を P の部分 R 加群といいます.

たとえば準同型写像 $f : P \to Q$ にたいして $\mathrm{Ker}(f)$ は P の, $\mathrm{Im}(f)$ は Q の部分加群です.

なぜなら s_1, $s_2 \in \mathrm{Ker}(f)$ にたいして $f(s_1 + s_2) = f(s_1) + f(s_2) = 0 + 0 = 0$ なので $s_1 + s_2 \in \mathrm{Ker}(f)$.

$s \in \mathrm{Ker}(f)$, $r \in R$ にたいして $f(rs) = rf(s) = r \times 0 = 0$ なので $rs \in \mathrm{Ker}(f)$ となるからです. $\mathrm{Im}(f)$ も同様に示せます.

P の部分 R 加群 S があると P のある部分集合の集合 $R/S = \{\, \overline{r} \mid \in R \,\}$ を考えられます. ここで $\overline{r} = \{\, r + r' \mid r' \in S \,\}$ と定義します（$r + S$ とかくこともある）. $\overline{r}$ は R の部分集合で r を $\overline{r}$ の代表元といいます. $\overline{r_1} = \overline{r_2} \iff r_1 - r_2 \in S$ が成り立ちます.

R/S は自然に R 加群となり, 商加群といいます.

加法 $\overline{r_1} + \overline{r_2} = \overline{r_1 + r_2}$.
R 倍 $r_1\overline{r_2} = \overline{r_1 r_2}$.

単位元は $\overline{0}$ です.

加法が well-defined であることを確認します. $\overline{r_1} = \overline{r_1'}$, $\overline{r_2} = \overline{r_2'}$ とします. すると $r_1 - r_1'$, $r_2 - r_2' \in S$. よって $(r_1 + r_2) - (r_1' + r_2') \in S$ となって $\overline{r_1 + r_2} = \overline{r_1' + r_2'}$. これは加法が代表元のとりかたに寄らずに定まることを意味します. R 倍も同様に示せます.

2.5 準同型定理

準同型写像 $f : P \to Q$ があると自然に

$$\begin{array}{rccc} \overline{f}: & P/\operatorname{Ker}(f) & \longrightarrow & Q \\ & \cup & & \cup \\ & \overline{p} & \longmapsto & f(p) \end{array}$$

を定義できます. $\overline{f}$ が well-defined なことだけを確認しましょう. $\overline{p} = \overline{p'}$ となる別の代表元 p' をとると $p - p' \in \operatorname{Ker}(f)$ なので $f(p) - f(p') = f(p - p') = 0$. よって $f(p) = f(p')$. $\overline{f}$ が R 加群として準同型であることも示せます.

$\operatorname{Ker}(\overline{f})$ はなんでしょうか. $\overline{f}(\overline{p}) = f(p) = 0$ なので

$$\operatorname{Ker}(\overline{f}) = \left\{ \overline{0} \right\}.$$

つまり $\overline{f}$ は単射です. 0 につぶれる元を同じものとみなすのだからある意味当然です.

定理 2.1 (準同型定理)**.** 準同型写像 $f : P \to Q$ があると, $\overline{f} : P/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ は同型になる.

2.6 完全系列

加群の列を考えます. 結構抽象度が高くなってくるのでちゃんと手を動かしてみてください.

R 加群 P_1, P_2, ... の列とその間の準同型写像 $f_1 : P_1 \to P_2$, $f_2 : P_2 \to P_3$, ... があったときに $\operatorname{Im}(f_i) = \operatorname{Ker}(f_{i+1})$ が成り立つときその列を完全（系）列（exact sequence）といいます.

たとえば

$$0 \xrightarrow{0_P} P \xrightarrow{f} Q$$

という完全列を考えます. 0 というのは単位元 0 のみからなる加群のことです. 0 から P の写像 0_P は 0 を 0 に写すものです. 最初なので明記しましたが普通省略します.

さて, 上記の列が完全であるということは $\operatorname{Im}(0_P) = \operatorname{Ker}(f)$ が成り立つということです. $\operatorname{Im}(0_P)$ は 0 なので $\operatorname{Ker}(f) = 0$ つまり f が単射であるということの言い換えにすぎません. 同様に

$$P \xrightarrow{f} Q \xrightarrow{0_Q} 0$$

という完全列を考えてみます. Q から 0 への写像 0_Q も Q の全ての元を 0 に写す写像しかないのでやはり通常は省略します. これが完全だということは $\operatorname{Im}(f) = \operatorname{Ker}(0_Q)$ ということです. 0_Q は Q の全ての元を 0 に写すのですから $\operatorname{Ker}(0_Q) = Q$ です. つまり $\operatorname{Im}(f) = Q$. これは f が全射であることの言い換えです. 単なる言葉遊びが続きますがもう一つ.

$$0 \to P \xrightarrow{f} Q \to 0$$

が完全だとどうなるでしょうか. $0 \to P \to Q$ が完全であることから f は単射, $P \to Q \to 0$ が完全であることから f は全射ということを意味しているので f は全単射, すなわち同型であるということの言い換えです.

ペアリングの定義で重要なのは次の完全列です.

$$0 \to M \xrightarrow{\psi} N \xrightarrow{\varphi} P \to 0 \tag{2}$$

これは φ が全射, ψ が単射, かつ $\operatorname{Im}(\psi) = \operatorname{Ker}(\varphi)$ であるということです. 特に $\varphi \circ \psi = 0$.

2.7 Hom の左完全性

前節の完全列と Hom との関連を考えてみましょう.

加群の間の写像があると Hom を作れました. 式**??**の他に加群 Q を考えます. そうすると $\varphi^* : \mathrm{Hom}(P, Q \to \mathrm{Hom}(N, Q)$ という写像を作れました. 同様に $\psi^* : \mathrm{Hom}(N, Q) \to \mathrm{Hom}(M, Q)$ という写像も作れます. 実は

定理 2.2.

$$M \xrightarrow{\psi} N \xrightarrow{\varphi} P \to 0$$

が完全列なら

$$0 \to \mathrm{Hom}(P, Q) \xrightarrow{\varphi^*} \mathrm{Hom}(N, Q) \xrightarrow{\psi^*} \mathrm{Hom}(M, Q)$$

が完全列となります.

完全列 $M \to N \to P \to 0$ に Hom を作用させて新しい完全列を作るので, これを $\mathrm{Hom}(, Q)$ の左完全性といいます.

証明しましょう. まず φ^* は単射です. なぜなら $f \in \mathrm{Hom}(P, Q)$ について $\varphi^*(f) = 0$ とします. これは任意の $n \in N$ について $\varphi^*(f)(n) = f(\varphi(n)) = 0$ ということですが, φ は全射なので（完全列の仮定）, $\varphi(n)$ は P の全ての値をとります. 全ての P の値について f が 0 ということは f は 0 写像ということです. つまり $f = 0$. $\varphi^*(f) = 0 \Leftrightarrow f = 0$ がいえたので φ^* は単射です.

次に $\psi^* \circ \varphi^* = 0$ を確認します.

任意の $f \in \mathrm{Hom}(P, Q), m \in M$ について,

$$\begin{aligned} \psi^* \circ \varphi^*(f)(m) &= \psi^*(f \circ \varphi)(m) \\ &= (f \circ \varphi \circ \psi)(m) \\ &= f(\varphi(\psi(m))) \\ &= 0 \qquad\qquad (\varphi \circ \psi = 0 \text{ なので}). \end{aligned}$$

これで $\mathrm{Im}(\varphi^*) \subseteq \mathrm{Ker}(\psi^*)$ が示せました.

最後, $\mathrm{Im}(\varphi^*) \supseteq \mathrm{Ker}(\psi^*)$ を示します. $f \in \mathrm{Ker}(\psi^*)$ をとります. つまり任意の $m \in M$ について

$$\psi^*(f)(m) = f(\psi(m)) = 0 \tag{3}$$

この条件の元で f が $\mathrm{Im}(\varphi^*)$ の元であること, すなわちある $g \in \mathrm{Hom}(P, Q)$ について $f = \varphi^*(g)$ を示す必要があります. 具体的に構成しましょう（ここで少し考えてみてください）.

任意の $p \in P$ について φ は全射なのである $n \in N$ があって $\varphi(n) = p$. このとき $g(p) := f(n)$ とします (実はこれ, 選択公理なんですが細かいことは気にしない). これは well-defined です（n のとり方に寄らず $g(p)$ が定まることを示す）. なぜなら他の $n' \in N$ で $\varphi(n') = p$ とすると $\varphi(n - n') = 0$. $\mathrm{Im}(\psi) = \mathrm{Ker}(\varphi)$ より, ある $m \in M$ があって $\psi(m) = n - n'$. すると式**??**の仮定により $f(n - n') = f(\psi(m)) = 0$. よって $f(n) = f(n')$.

まだ $g : P \to Q$ を構成しただけで, $g \in \mathrm{Hom}(P, Q)$ を示したわけではありませんが, それは g の作り方から容易に示せます. 以上で $\mathrm{Im}(\varphi^*) = \mathrm{Ker}(\psi^*)$ となり完全性の証明が終わりました.

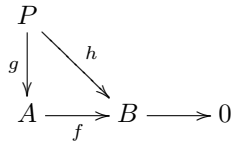
実は Hom の*左*完全性という名前の示す通り, 右完全ではありません. つまり ψ^* は全射になるとは限らないのです. そこでどれぐらいずれてるかの調整のために Ext というものを考えます.

2.8 Ext の定義のための準備

しばらく Ext の定義のためのホモロジー代数の用語と基本的な定理を証明し続けます. 面倒だと思う人はさくっと Ext まで飛ばしてください.

2.9 射影加群と射影分解

R 加群 P が射影的であるとは任意の R 加群 A, B と全射準同型写像 $f : A \to B$, 準同型写像 $h : P \to B$ があったとき, ある準同型写像 $g : P \to A$ があって $h = f \circ g$ とできるときをいいます.



この初見ではどうみても作為的な定義が, 加群のコホモロジーの定義に絶大な威力を発揮します.

たとえば R は自身を R 加群と思うと射影的です. なぜなら $f : A \to B \to 0$, $h : R \to B$ があったとします. $r \in R$ について $h(r) = rh(1)$. f は全射なのである $a \in A$ があって $f(a) = h(1)$. $g : R \to A$ を $g(r) = ra$ と定義すると $h(r) = rf(a) = f(ra) = f(g(r))$ が成り立つからです.

R の元を並べて作った直和 $\oplus R$ 自由加群といいますが, 同様にして射影的であることを示せます.

さて, R 加群 P にたいして P の P 個の直和 $P_0 = \bigoplus_{\lambda \in P} R$ を考えて λ 番目を λ, それ以外を 0 に写す写像 ε を考えるとこれは全射です.

その $\mathrm{Ker}(\varepsilon)$ にたいして同じことを繰り返すと $d_1 : P_1 \to \mathrm{Ker}(\varepsilon) \to 0$ を作れます. $\mathrm{Ker}(\varepsilon)$ は P_0 の部分群なので $\mathrm{Im}(d_0) = \mathrm{Ker}(\varepsilon)$. この操作を繰り返すことで

$$\ldots \to P_n \underset{d_n}{\longrightarrow} P_{n-1} \to \cdots \underset{d_1}{\longrightarrow} P_0 \underset{\varepsilon}{\to} P \to 0$$

という完全列を作れます.

より一般に R 加群 P にたいして, （自由加群とは限らない）射影加群の列 $\{ P_n \}$ とその間の準同型 $\{ d_n \}$ が存在し,

$$\ldots \to P_n \underset{d_n}{\longrightarrow} P_{n-1} \to \cdots \to P_0 \underset{\varepsilon}{\to} P \to 0$$

が完全列であるとき, (P_n, d_n, ε) を P の射影分解といいます. 自由加群は射影加群なので上記の操作により射影分解は常に存在します.

R が単項イデアル整域（PID）と呼ばれる都合のよい環であるとき（例えば $\mathbb{Z}$ や $\mathbb{Z}/p\mathbb{Z}$）, 自由加群の部分加群はまた自由加群, つまり射影加群になることが知られています.

（注意）R が PID のとき, 自由であることと射影的であることは同値です.

つまり, 上記の $\mathrm{Ker}(\varepsilon)$ が射影的になり, そこで止まります. 言い直すと R が PID なら任意の R 加群 P について $0 \to P_1 \to P_0 \to P \to 0$ という射影分解が存在します. とりあえず, これを事実として進めましょう.

2.10　ホモロジー

R 加群の列とその間の準同型写像の組 $X = \{ X_n, d_n : X_n \to X_{n-1} \}$ が $d_n \circ d_{n+1} = 0$ を満たすとき, X を鎖複体（chain complex）といいます.

$$\ldots \to X_{n+1} \xrightarrow{d_{n+1}} X_n \xrightarrow{d_n} X_{n-1} \to \ldots$$

このとき $Z_n(x) = \mathrm{Ker}(d_n)$, $B_n(X) = \mathrm{Im}(d_{n+1})$ として $H_n(X) = Z_n(X)/B_n(X)$ を X の n 次ホモロジーといいます.

$d_n \circ d_{n+1} = 0$ から $\mathrm{Im}(d_{n+1}) \subseteq \mathrm{Ker}(d_n)$ なので完全列は鎖複体ですがその逆は一般には成り立ちません. 完全列のホモロジーは $Z_n(X) = B_n(X)$ なので 0 です.

二つの鎖複体 $X = \{ X_n, d_n \}$, $Y = \{ Y_n, e_n \}$ とその間の準同型写像の組 $f_n : X_n \to Y_n$ が $\{ d_n \}$ と可換なとき（すなわち $f_{n-1} \circ d_n = e_n \circ f_n$） $f = \{ f_n \}$ を複体写像といいます.

$$\begin{array}{ccccccccc}
\ldots & \longrightarrow & X_{n+1} & \xrightarrow{d_{n+1}} & X_n & \xrightarrow{d_n} & X_{n-1} & \longrightarrow & \ldots \\
 & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\
\ldots & \longrightarrow & Y_{n+1} & \xrightarrow[e_{n+1}]{} & Y_n & \xrightarrow[e_n]{} & Y_{n-1} & \longrightarrow & \ldots
\end{array}$$

$Z_n(X) = \mathrm{Ker}(d_n) \ni x$ について可換性の条件から, $e_n(f_n(x)) = f_{n-1}(d_n(x)) = 0$ となり $f_n(x) \in \mathrm{Ker}(e_n)$. つまり $f_n(Z_n(X)) \subseteq Z_n(Y)$.

また $X_{n+1} \ni x$ について $f_n(d_{n+1}(x)) = e_{n+1}(f_{n+1}(x))$. つまり $f_n(B_n(X)) \subseteq B_n(Y)$. よって, $H(f_n) : H_n(X) \to H_n(Y)$ を自然に定義できます.

2.11　ホモトピー

$X = \{ X_n, d_n \}$, $Y = \{ Y_n, e_n \}$ を鎖複体, $f = \{ f_n \}$, $g = \{ g_n \}$ を X から Y への 2 個の鎖準同型とします.

f と g が鎖ホモトープであるとは, ある R 準同型写像 $s = \{ s_n : X_n \to Y_{n+1} \}$ があって,

$$f_n - g_n = s_{n-1} \circ d_n + e_{n+1} \circ s_n$$

となるものをいいます.

$$\begin{array}{ccccccccc}
\ldots & \longrightarrow & X_{n+1} & \xrightarrow{d_{n+1}} & X_n & \xrightarrow{d_n} & X_{n-1} & \longrightarrow & \ldots \\
 & & \downarrow & \swarrow{\scriptstyle s_n} & \downarrow{\scriptstyle f_n, g_n} & \swarrow{\scriptstyle s_{n-1}} & \downarrow & & \\
\ldots & \longrightarrow & Y_{n+1} & \xrightarrow[e_{n+1}]{} & Y_n & \xrightarrow[e_n]{} & Y_{n-1} & \longrightarrow & \ldots
\end{array}$$

f と g の差が右行って左斜め下に行くものと左斜めに行って右にいくものとの和でかけるということです.

鎖ホモトープという条件は同値関係 $\sim$ になります. $Z_n(X) \ni x$ にたいして

$$f_n(x) - g_n(x) = (s_{n-1} \circ d_n + e_{n+1} \circ s_n)(x) = e_{n-1}(s_n(x)) \in B_n(Y).$$

よって $H(f_n)(x) = H(g_n)(x)$. つまり $f \sim g$ なら $H(f) = H(g)$ となります.

鎖複体 X, Y にたいして鎖準同型 $f : X \to Y$, $g : Y \to X$ が存在して $g \circ f \sim \mathrm{id}_X$, $f \circ g \sim \mathrm{id}_Y$ となったとします（id_X などは恒等写像）. この状態を X と Y は同じホモトピー型を持つといいます. すると

$$H(g) \circ H(f) = H(g \circ f) = H(\mathrm{id}_X) = 1, H(f) \circ H(g) = H(f \circ g) = H(\mathrm{id}_Y) = 1$$

となり, $H_n(X)$ と $H_n(Y)$ は同型となります.

2.12 コホモロジー

ホモロジーの添え字の変化を反対にして作ったものがコホモロジーです. R 加群の列とその間の準同型写像の組 $X = \left\{ X^n, d^n : X^n \to X^{n+1} \right\}$ が $d^{n+1} \circ d^n = 0$ を満たすとき, X を双対鎖複体（dual chain complex）といいます.

$$\ldots \to X^{n-1} \xrightarrow{d^{n-1}} X^n \xrightarrow{d^n} X^{n+1} \to \ldots$$

このとき, $Z^n(x) = \mathrm{Ker}(d^n)$, $B^n(X) = \mathrm{Im}(d^{n-1})$ として $H^n(X) = Z^n(X)/B^n(X)$ を X の n 次コホモロジーといいます.

二つの双対鎖複体 $X = \{ X^n, d^n \}$, $Y = \{ Y^n, e^n \}$ とその間の準同型写像の組 $f^n : X^n \to Y^n$ が $\{ d^n \}$ と可換なとき（すなわち $f^{n+1} \circ d^n = e^n \circ f^n$） $f = \{ f^n \}$ を双対複体写像といいます.

$$\begin{array}{ccccccccc}
\ldots & \longrightarrow & X^{n-1} & \xrightarrow{d^{n-1}} & X^n & \xrightarrow{d^n} & X^n & \xrightarrow{d^{n+1}} & \ldots \\
 & & \downarrow{\scriptstyle f^{n-1}} & & \downarrow{\scriptstyle f^n} & & \downarrow{\scriptstyle f^{n+1}} & & \\
\ldots & \longrightarrow & Y^{n-1} & \xrightarrow[e^{n-1}]{} & Y^n & \xrightarrow[e^n]{} & Y^n & \xrightarrow[e^{n+1}]{} & \ldots
\end{array}$$

可換性の条件からホモロジーと同様に $f^n(Z^n(X)) \subseteq Z^n(Y)$, $f^n(B^n(X)) \subseteq B^n(Y)$ が成り立ちます. よって $H(f^n) : H^n(X) \to H^n(Y)$ を自然に定義できます. ホモトピーも同様にできます.

2.13 射影分解の一意性

射影分解はある種の一意性を持ちます. P と P' の射影分解を $(P_n, d_n, \varepsilon), (P'_n, d'_n, \varepsilon')$ とします.

$$\begin{array}{ccccccccccc}
\ldots & \longrightarrow & P_n & \xrightarrow{d_n} & P_{n-1} & \longrightarrow & \ldots & \xrightarrow{d_1} & P_0 & \xrightarrow{\varepsilon} & P & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi_n} & & \downarrow{\scriptstyle \phi_{n-1}} & & & & \downarrow{\scriptstyle \phi_0} & & \downarrow{\scriptstyle \phi} & & \\
\ldots & \longrightarrow & P'_n & \xrightarrow[d'_n]{} & P'_{n-1} & \longrightarrow & \ldots & \xrightarrow[d'_1]{} & P'_0 & \xrightarrow[\varepsilon']{} & P' & \longrightarrow & 0
\end{array}$$

$\mathrm{Hom}(P, P') \ni \phi$ を一つとります. $\varepsilon' : P'_0 \to P \to 0$ という全射と $\phi \circ \varepsilon : P_0 \to P$ という写像を考えると, P'_0 の射影性から, ある $\phi_0 : P_0 \to P'_0$ で $\phi \circ \varepsilon = \varepsilon' \circ \phi_0$ を満たすものが存在します.

すると

$$\varepsilon' \circ \phi_0 \circ d_1 = \phi \circ \varepsilon \circ d_1 = \phi \circ 0 = 0$$

より

$$\mathrm{Im}(\phi_0 \circ d_1) \subseteq \mathrm{Ker}(\varepsilon') = \mathrm{Im}(d'_1).$$

よって $d'_1 : P'_1 \to \mathrm{Im}(d'_1) \to 0$ という全射と $\phi_0 \circ d_1 : P_1 \to \mathrm{Im}(d'_1)$ という写像にたいして, P'_1 の射影性から $\phi_1 : P_1 \to P'_1$ で $d'_1 \circ \phi_1 = \phi_0 \circ d_1$ であるものが存在します. これを繰り返すことで上記図式を可換にする鎖写像 $\{\phi_n\}$ を構成できます. $\{\phi_n\}$ を ϕ の持ち上げということにしましょう.

$g_n = \phi_n - \phi'_n$ としましょう. これは $\phi - \phi = 0$ 写像の持ち上げとなっています. $s_{-1} = 0$ として, $s_0 : P_0 \to P'_1$ を構成します.

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & P_n & \xrightarrow{d_n} & P_{n-1} & \longrightarrow & \cdots & \xrightarrow{d_1} & P_0 & \xrightarrow{\varepsilon} & P & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle g_n} & & \downarrow{\scriptstyle g_{n-1}} & & & & \downarrow{\scriptstyle g_0} & & \downarrow{\scriptstyle 0} & & \\
\cdots & \longrightarrow & P'_n & \xrightarrow[d'_n]{} & P'_{n-1} & \longrightarrow & \cdots & \xrightarrow[d'_1]{} & P'_0 & \xrightarrow[\varepsilon']{} & P' & \longrightarrow & 0
\end{array}$$

$d'_0 \circ g_0 = d_0 \circ 0 = 0$ より $\mathrm{Im}(g_0) \subseteq \mathrm{Ker}(d'_0) = \mathrm{Im}(d'_1)$. よって全射 $d'_1 : P'_1 \to \mathrm{Im}(d'_1)$ と $g_0 : P_0 \to \mathrm{Im}(d'_1)$ にたいして P'_1 の射影性から, $s_0 : P_0 \to P'_1$ で $g_0 = d'_1 \circ s_0$ であるものが存在します.

次に, $d'_1 \circ (g_1 - s_0 \circ d_1) = d'_1 \circ g_1 - g_0 \circ d_1 = 0$ より $g_1 - s_0 \circ d_1 \subseteq \mathrm{Ker}(d'_1) = \mathrm{Im}(d'_2)$. P'_2 の射影性から $s_1 : P_1 \to P'_2$ で $s_1 \circ d'_2 = g_1 - s_0 \circ d_1$ であるものが存在します. つまり $g_1 = s_1 \circ d'_2 + s_0 \circ d_1$. これを繰り返すことで $\{s_n\}$ を構成できます. よって $\{\phi_n\} \sim \{\phi'_n\}$. **??**節から $H(\phi_n) = H(\phi'_n)$ となり, $H(\phi^\star)$ は ϕ の持ち上げかたによらないことが分かります.

長い準備の前半が終わりました.

2.14 Ext

漸く Ext の定義にたどり着きました. R 加群 P, Q にたいして Ext を次のように定義します. P の射影分解 (P_n, d_n, ε)

$$\ldots \to P_n \underset{d_n}{\longrightarrow} P_{n-1} \to \ldots \to P_0 \underset{\varepsilon}{\to} P \to 0$$

を一つとり, $d_0 = 0$ として $X = \{\mathrm{Hom}(P_n, Q), d_{n^\star}\}$ を考えます (P を取り除きます). この鎖複体にたいして $\mathrm{Hom}(, Q)$ を適用すると $0 \to \mathrm{Hom}(P_0, Q) \to \mathrm{Hom}(P_1, Q) \to \ldots$ という双対鎖複体を構成でき, このコホモロジーを Ext とします. つまり

$$\mathrm{Ext}^n(P, Q) := H^n(\mathrm{Hom}(P_\star, Q))$$

で定義します.

$\varepsilon^\star : \mathrm{Hom}(P, Q) \to \mathrm{Hom}(P_0, Q)$ は単射なので $\mathrm{Ext}^0(P, Q) = \mathrm{Ker}(d_{0^\star}) = \mathrm{Im}(\varepsilon^\star) = \mathrm{Hom}(P, Q)$ が成り立ちます.

R が PID のとき,**??**節の最後に書いたように

$$0 \to P_1 \underset{d}{\to} P_0 \underset{\varepsilon}{\to} P \to 0$$

という射影分解にたいして Ext を考えられます. そうすると

$$0 \to \mathrm{Hom}(P_0, Q) \underset{d^\star}{\longrightarrow} \mathrm{Hom}(P_1, Q) \underset{0^\star}{\longrightarrow} 0$$

という鎖複体なので

$$\mathrm{Ext}^1(P, Q) = \mathrm{Ker}(0^\star)/\,\mathrm{Im}(d^\star) = \mathrm{Hom}(P_1, Q)/\,\mathrm{Im}(d^\star) = \mathrm{Coker}(d^\star),$$
$$\mathrm{Ext}^n(P, Q) = 0 \text{ for } n \geq 2$$

となります.

ここで, Silverman の論文に出てくる Ext の表現との関係を見てみましょう. Silverman のところでは

$$\begin{array}{l}\mathrm{Ext}(P,Q)\text{ の元 }f\text{ は }f:P\times P\to Q\text{ で,}\\ f(x,y)-f(x,y+z)-f(x+y,z)-f(y,z)=0\text{ を満たすもの.}\\ \text{ただし, }f\sim f'\Leftrightarrow\text{ある }g:P\to Q\text{ で }(f-f')(x,y)=g(x+y)-g(x)-g(y)\end{array}\tag{4}$$

でした.

きちんとした定義の $\mathrm{Ext}^1(P,Q)$ の元がそのように表現できることを示します. ε が全射なので $\sigma:P\to P_0$ で $\varepsilon(\sigma(p))=p$ となる σ をとることが出来ます. この σ は準同型である必要はありません.

$x,y\in P$ にたいして

$$\varepsilon(\sigma(x+y)-\sigma(x)-\sigma(y))=(\varepsilon\circ\sigma)(x+y)-(\varepsilon\circ\sigma)(x)-(\varepsilon\circ\sigma)(y)=0.$$

つまり $\sigma(x+y)-\sigma(x)-\sigma(y)\in\mathrm{Ker}(\varepsilon)=\mathrm{Im}(d)$. よって $z\in P_1$ の元で $d(z)=\sigma(x+y)-\sigma(x)-\sigma(y)$ となるものが唯一定まります. この対応を $\lambda(x,y)=z$ とかくことにします.

$$\begin{aligned}&\lambda:P\times P\to P_1,\\ &d(\lambda(x,y))=\sigma(x+y)-\sigma(x)-\sigma(y).\end{aligned}$$

$\mathrm{Ext}^1(P,Q)$ の元の代表 $f\in\mathrm{Hom}(P_1,Q)$ をとってきて, この λ との合成 $\tilde{f}=f\circ\lambda$ を考えると $\tilde{f}:P\times P\to Q$ で $f(x,y)-f(x,y+z)+f(x+y,z)-f(y,z)=0$ となることがすぐわかります.

また, $\mathrm{Im}(d^\star)$ の元は $g:P_0\to Q$ を用いて $g\circ d:P_1\to Q$ で表せます. よって,

$$\widetilde{(g\circ d)}(x,y)=g\circ d(\lambda(x,y))=g(\sigma(x+y)-\sigma(x)-\sigma(y)).$$

つまり $f'=g\circ\sigma$ とおくと $\widetilde{(g\circ d)}(x,y)=g'(x+y)-g'(x)=g'(y)$ となります.

というわけで $\mathrm{Ext}^1(P,Q)$ の元を自然に式**??**の形とみなすことが出来ました（もちろん全射にはならない）.

2.15 Ext の完全列

R が PID のとき, $\mathrm{Ext}^n=0$ $(n\geq 2)$ なので Ext^1 を Ext と略記して話を進めます.

定理 2.3. R を PID とする.

$$0\to M\xrightarrow{\psi}N\xrightarrow{\phi}P\to 0$$

が R 加群の完全列のとき,

$$0\to\mathrm{Hom}(P,Q)\to\mathrm{Hom}(N,Q)\to\mathrm{Hom}(M,Q)\to\mathrm{Ext}(P,Q)\to\mathrm{Ext}(N,Q)\to\mathrm{Ext}(M,Q)\to 0$$

は完全列である.

（注意）R が一般の環のときは最後が 0 ではなくずっと Ext の列が続きます.

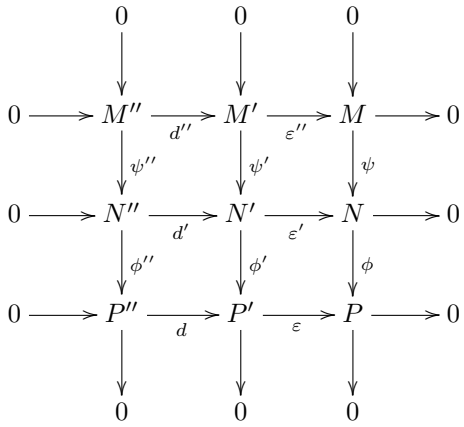
証明しましょう. またしばらくかかるので位相空間などまで飛ばして下さい. ここからしばらく R が PID であることを仮定します. この仮定は殆どのところで不要, あるいは数学的帰納法を用いて証明できます. 図式が煩雑になるため省略します.

2.16 補題 1

補題 1. R を PID とする. M と P の射影分解をそれぞれ $(\{M', M''\}, d'', \varepsilon'')$, $(\{P', P''\}, d, \varepsilon)$ とします. このとき,

$$0 \to M' \to N' \to P' \to 0$$

が完全になるような N の射影分解 $(\{N', N''\}, d', \varepsilon')$ が存在し, 下記図式が全て可換になるようにできます.



1. N', ε' **の定義** $N' := M' + P'$ とします. さらに

$$\pi : N' = M' + P' \ni (m', p') \to m' \in M',$$
$$\iota : P' \ni p' \to (0, p') \in N'$$

とします. すると $0 \to M' \to N' \to P' \to 0$ は完全. $\pi \circ \psi' = \mathrm{id}_{M'}$. $\phi' \circ \iota = \mathrm{id}_{P'}$.
全射 $\phi : N \to P$ と $\varepsilon : P' \to P$ と P' の射影性からある $f : P' \to N$ で $\varepsilon = \phi \circ f$ となるものが存在.
$\varepsilon' : N' \to N$ を $\varepsilon' = \psi \circ \varepsilon'' \circ \pi + f \circ \phi'$ とします.

2. **可換性** $\varepsilon' \circ \psi' = \psi \circ \varepsilon'' \circ \pi \circ \psi' + f \circ \phi' \circ \psi' = \psi \circ \varepsilon''$. $\phi \circ \varepsilon' = \phi \circ \psi \circ \varepsilon'' \circ + \phi \circ f \circ \phi' = \varepsilon \circ \phi'$

3. ε' **の全射性** $n \in N$ をとる. ε が全射なので

$$\exists p' \in P' \text{ s.t. } \varepsilon(p') = \phi(n).$$
$$\phi(n - \varepsilon'(\iota(p'))) = \varepsilon(p') - \varepsilon \circ \phi' \circ \iota(p') = \varepsilon(p') - \varepsilon(p') = 0.$$

よって

$$\exists m \in M \text{ s.t. } \psi'(m') = n - \varepsilon'(\iota(p')).$$

ε'' が全射なので

$$\exists m' \in M' \text{ s.t. } \varepsilon''(m') = m.$$

よって

$$\begin{aligned}\varepsilon'(\psi'(m')) + \iota(p') &= \psi \circ \varepsilon'' \circ \pi\psi'(m') + f \circ \phi'\psi'(m') + \varepsilon'(\iota(p')) \\ &= \psi \circ \varepsilon''(m') + \varepsilon'(\iota(p')) = \psi(m) + \varepsilon'(\iota(p')) = n.\end{aligned}$$

4. (M, N, P) の代わりに今構成した (M', N', P') の部分加群 $(\mathrm{Ker}(\varepsilon''), \mathrm{Ker}(\varepsilon'), \mathrm{Ker}(\varepsilon))$ を置き換えることで N'' を構成できます.

5. $d' : N'' \to \mathrm{Ker}(\varepsilon')$ が単射であること. $d'(n'') = 0$ とする.

$$d(\phi''(n'')) = \phi'(d'(n'')) = 0.$$

d は単射なので $\phi''(n'') = 0$. よって

$$\exists m'' \in M'' \text{ s.t. } \psi''(m'') = n'',$$
$$\psi' \circ d''(m'') = d' \circ \psi''(m'') = d'(n'') = 0.$$

ψ', d'' が単射なので $m'' = 0$. よって $n'' = 0$. R が PID でない場合は左の $0 \to$ が無くて必要なだけ繰り返して延ばします.

2.17 分解型完全列

$\mathrm{Hom}(, Q)$ の右が完全になるときがあります.

補題 2. （R は PID でなくてよい）R 加群 M, N, P に対する完全列があり, $\tau \circ i = \mathrm{id}_M$ とすると, R 加群 Q にたいして

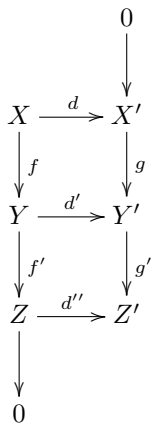
$$0 \to M \underset{\tau}{\overset{i}{\rightleftarrows}} N \to P \to 0$$
$$\Rightarrow 0 \to \mathrm{Hom}(P, Q) \to \mathrm{Hom}(N, Q) \to \mathrm{Hom}(M, Q) \to 0 \quad \text{（完全）}$$

上記のような τ があるとき分解型完全列といいます. そうでないときも最後の $\to 0$ 以外は成り立つのでそこを示します. といっても簡単で, $\mathrm{Hom}(M, Q) \ni f$ について, $f \circ \tau \in \mathrm{Hom}(N, Q)$ を考えると $i^\star(f \circ \tau) = f \circ \tau \circ i = f$.

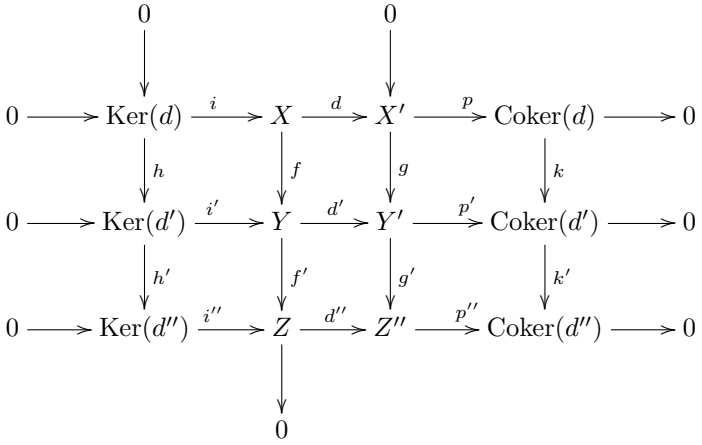
2.18 ヘビの補題

（R は PID でなくてよい）

補題 3 (ヘビの補題)**.** 次の完全列があったときに少し長い完全列を作れます. X, Y, Z, X', Y', Z' が R 加群で



があったときに, $\mathrm{Ker}, \mathrm{Coker}$ を下記のように増やせてかつ $\mathrm{Ker}(d'') \to \mathrm{Coker}(d)$ をつなげられます.

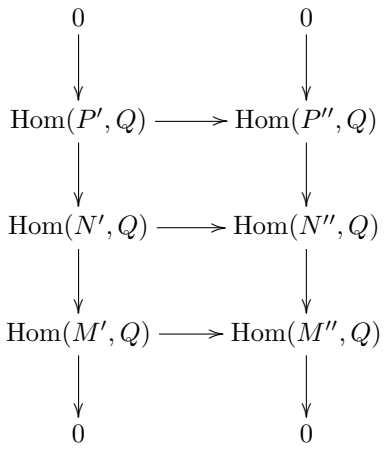


$$0 \to \mathrm{Ker}(d) \to \mathrm{Ker}(d') \to \mathrm{Ker}(d'') \underset{\delta}{\to} \mathrm{Coker}(d) \to \mathrm{Coker}(d') \to \mathrm{Coker}(d'') \to 0 \text{（完全）}$$

1. $(i, i', i'', p, p', p''$ の構成)
   $\mathrm{Ker}(d)$ は X の部分加群なので標準的な inclusion です. 他も同様です. $\mathrm{Coker}(d) = X'/\mathrm{Im}(d)$ なので p は標準的な projection です.
2. (h の構成)
   $\mathrm{Ker}(d) \ni x$ について $d' \circ f \circ i(x) = g \circ d(x) = 0$ より $f \circ i(x) \in \mathrm{Ker}(d')$. つまり f を $\mathrm{Ker}(d)$ に制限した写像 h は $h : \mathrm{Ker}(d) \to \mathrm{Ker}(d')$ になります. h' も同様です.
3. ($\delta : \mathrm{Ker}(d'') \to \mathrm{Coker}(d)$ の構成)
   δ を連結写像といいます. $\mathrm{Ker}(d'') \ni x$ にたいして f' が全射なので $\exists y \in Y$ s.t. $f'(y) = i''(x)$. $g'(d'(y)) = d''(f'(y)) = d''(i''(x)) = 0$ より $d'(y) \in \mathrm{Ker}(g') = \mathrm{Im}(g)$. よって $x' \in X'$ で $g(x') = d'(y)$ となるものがただ一つ存在します. $\delta(x) := p(x')$ としましょう.
   well-defined を確認します. 別の $\tilde{y} \in Y$ s.t. $f'(\tilde{y}) = i''(x)$ があったとすると, $f'(\tilde{y} - y) = 0$. よって $\exists x \in X$ s.t. $f(x) = \tilde{y} - y$. $\tilde{x'} \in X'$ で $g(\tilde{x'} - x' = d(x)$. よって $p(\tilde{x'}) = p(x')$ となり δ は well-defined になります. 他の完全性の部分は略.

2.19 定理の証明

準備が整いました. さて PID な環 R の完全列 $0 \to M \to N \to P \to 0$ があったときに, 補題 1 から完全列を作り, それにたいして $\mathrm{Hom}(, Q)$ を作用させます. 真ん中の縦の列は分解型完全列なので補題 2 を使うと次の図式がでます.



これにたいしてヘビの補題を適用することで Ker と Coker の完全列ができます. ところで $\mathrm{Ker}(d^\star)$ は $\mathrm{Hom}(P,Q)$, Coker は Ext なので, 結局

$$0 \to \mathrm{Hom}(P,Q) \to \mathrm{Hom}(N,Q) \to \mathrm{Hom}(M,Q) \to \mathrm{Ext}(P,Q) \to \mathrm{Ext}(N,Q) \to \mathrm{Ext}(M,Q) \to 0$$

が完全となりました. 大変だった.

3 多様体

ホモロジー代数の話はひとまずそれぐらいにして, 次に位相空間まわりの最低限の定義を復習しておきます. またもや無味乾燥な定義の列...

3.1 位相空間

実数や複素数上の開集合は直感的ですが, 距離の定義できない空間でも遠い, 近いという概念を考えたいときに抽象的な位相空間が定義されました.

集合 X とその部分集合の族 Y の組 (X,Y) が位相空間であるとは

1) $X \in Y, \phi \in Y$
2) $U_1, U_2 \in Y$ について $U_1 \cap U_2 \in Y$
3) 任意個の $U_\lambda \in Y$ について $\bigcup_{\lambda\in\Lambda} U_\lambda \in Y$

を満たすものをいい, Y の元を X の開集合といいます. 開集合の補集合が閉集合です.

言葉で書くと, 全体と空集合は open, 有限個の open set の交わりは open, 無限個でもいい任意個の open set の併合は open ということです.

$Y = \{ X, \phi \}$ と開集合が 2 個しか無いときでも X は位相空間になります. 逆に Y を X 全ての部分集合としたときも X は位相空間になります. R の普通の開集合は開区間 (a,b) を組み合わせてできたものです. 無限個の開区間 $(1-\frac{1}{n}, 1+\frac{1}{n})$ の交わりは $\bigcap(1-\frac{1}{n}, 1+\frac{1}{n}) = \{1\}$ となり開集合ではありません. 上記定義の 2) が有限個なのはそれを反映しています. 代数多様体で定義される Zariski 位相はそれよりもずっと開集合が少ない感じです.

関数の連続性　位相空間 X, Y があったときに関数 $f : X \to Y$ が連続であるとは, Y の任意の開集合 U の引き戻し $f^{-1}(U)$ が X の開集合なときにいいます. この定義は抽象的ですが, X が実数や複素数上の関数の素朴な連続の定義に一致します.

コンパクト　位相空間 X の部分集合 K がコンパクトであるとは, K の任意の開被覆

$$\bigcup^{n} U_{\lambda_i} \supseteq K.$$

があったときに, そこから有限個取り出して覆えることです. X が実数などの距離空間のときはコンパクトは有界閉集合に一致します.

位相空間の連続写像 $f : X \to Y$ とコンパクト $K \subseteq X$ があったとき $f(K)$ はコンパクトです.

なぜなら $f(K)$ の開被覆があったとすると, それを f で引き戻せば K の開被覆になり, K はコンパクトなので有限個取れるからです.

Hausdorff　X が Hausdorff であるとは X の任意の異なる 2 点 x, y にたいして $U \in x, V \in y$ となる開集合 U, V があって $U \cap V = \phi$ とできることです. 要はどんなに近い 2 点であってもそれを分ける小さな開集合があるということです.

X が Hausdorff であることは $\Delta := \{ (x, x) \mid x \in X \}$ が $X \times X$ の中で closed であることと同値です. Zariski 位相は Hausdorff ではないのですが, Hausdorff 的な条件が必要なときに対角写像が"閉"であるという性質を使ってその代わりにすることがあります.

同相　$f : X \to Y$ が同相 (homeomorphic) 写像であるとは f が連続で, 逆写像 f^{-1} が存在して f^{-1} も連続なことです. 位相空間として同一視できるということです.

3.2　複素多様体

複素多様体とは大雑把にいうと局所的に $\mathbb{C}^n$ の開集合と思えて, それの貼りあわせたものであり, つなぎ目も滑らかになっているものです.

複素 1 変数関数 f がある開集合 D の各点で微分可能なとき D で正則（holomorphic）といいます. それは各点 z の近傍（z を含む開集合）で Taylor 展開できることと同値です. $\mathbb{C}$ 上正則で有界な関数は定数関数しかありません（Liouville の定理）. Cauchy の積分定理から示せます.

Hausdorff 空間 X が n 次元多様体であるとは X の開被覆 $X = \bigcup_{\lambda \in \Lambda} U_\lambda$ と各開被覆 U_λ にたいして $\mathbb{C}^n$ の開集合への同相写像 $\phi_\lambda : U_\lambda \to \phi_\lambda(U_\lambda) \subseteq \mathbb{C}^n$ があって $U_\lambda \cap U_\mu \neq \phi$ のとき $\phi_\mu \circ \phi_\lambda^{-1} : \phi_\lambda(U_\lambda \cap U_\mu) \to \phi_\mu(U_\lambda \cap U_\mu)$ が正則関数, かつ逆写像も正則関数であるものです.

言葉にするとややこしいですが, 図を書いてみると貼りあわせの感覚が分かると思います. $(U_\lambda, \phi_\lambda)$ を局所座標といいます.

X 上の関数 f が正則（holomorphic）であるとは, 局所座標を通じて作った $f \circ \phi_\lambda^{-1} : \phi_\lambda(U_\lambda) \to \mathbb{C}$ が正則なときにいいます.

3.3　射影空間

複素多様体の一例で重要な概念である射影空間を定義します.

Euclid 空間 $\mathbb{C}^{n+1}$ の原点でない 2 点 x, y に同値関係を「$x \sim y \Leftrightarrow$ ある $\lambda \in \mathbb{C}^*$ があって $x = \lambda y$」でいれます. ベクトルの向きが同じ点を同一視するということです. 同値関係で割った空間を

$$\mathbb{P}^n = \mathbb{C}^{n+1} \setminus \{\, 0 \,\}/\sim$$

と書き, n 次射影空間といいます. $\mathbb{P}^n$ は複素多様体になります. $x = (x_0, \ldots, x_n)$ の同値類を $(x_0 : \cdots : x_n)$ と書くことにします.

$\mathbb{P}^1$ で考えてみましょう. $U = \left\{ (x:y) \in \mathbb{P}^1 \,\middle|\, y \neq 0 \right\}$, $\phi : U \to \mathbb{C}$ を $\phi(x:y) = x/y$ とすると, ϕ は well-defined で 1 対 1 の対応になります. $\mathbb{P}^1 = U \cup V$ であり, $U \cap V$ では $\mathbb{C}^*$ と 1 対 1 の対応が付くこともわかって局所座標になります. $\mathbb{P}^1 - U = \left\{ (x:y) \in \mathbb{P}^1 \,\middle|\, y = 0 \right\}$ は $\{\, (1:0) \,\}$ と 1 点になります. これを ∞ とかくことにすると $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$ となります. Riemann 球面といいます.

複素多様体 X から $\mathbb{P}^1$ への正則な写像を X 上の有理型関数といいます. X 上の有理型関数全体を $M(X)$ と書くことにします.

3.4 アーベル多様体

アーベル多様体を定義します. といっても大雑把な所でお茶を濁します. とりあえず $\mathbb{C}$ 上の話で進めます.

V を g 次元複素ベクトル空間, Λ を $2g$ 次元 Z ベクトル空間として $X = V/\Lambda$ を g 次元複素トーラスといいます. 複素トーラスには自然に足し算の構造が入ります.

V の基底を $e_1, \ldots, e_g$, Λ の基底を $\lambda_1, \ldots, \lambda_{2g}$ として, $\lambda_i = \lambda_{1i}e_1 + \ldots + \lambda_{gi}e_g$ $(\lambda_{ji} \in \mathbb{C})$ とかいたとき g 行 $2g$ 列の行列 $\Pi = (\lambda_{ji})$ を周期行列といいます.

複素トーラス X の周期行列 Π にたいしてある非退化交代行列 $A \in M_{2g}(Z)$ $(A = -{}^tA)$ が存在して,

1) $\Pi A^{-1}\ {}^t\Pi = 0$
2) $i\Pi A^{-1}\ {}^t\tilde{\Pi} > 0$ （正定置 := 行列の固有値が全て正）

が成り立つとき X を複素アーベル多様体といいます.

1 次元のときは複素トーラスは必ずアーベル多様体になります. なぜなら Λ の基底を 1 と λ（実数でない）として, 非退化な交代行列 A について逆行列 A^{-1} を

$$A^{-1} = \begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}$$

とおくと 1) の条件は $(1\ \lambda)\ {}^t(b\lambda\ \ -b) = b\lambda - b\lambda = 0$. 2) の条件は $i(1\ \lambda)\ {}^t(b\tilde{\lambda}\ \ -b)\ 2b\ \mathrm{Im}(\lambda) > 0$ となり常に成り立つようにできるからです.

3.5 楕円曲線

1 次元複素トーラス（=1 次元アーベル多様体）を楕円曲線といいます.

$\pi : \mathbb{C} \to X := \mathbb{C}/\Lambda$ を $\pi(x) := x \mod \Lambda$ とします. 単に Λ だけずれた値を同一視するということです.

楕円曲線 X に位相を入れましょう. 「$U \subseteq X$ が open $\Leftrightarrow$ $\pi^{-1}(U)$ が $\mathbb{C}$ の中で open」と定義します. 更に $\pi : \mathbb{C} \to X$ は連続になります（ほぼ自明）.

X は Hausdorff です. まあこれも容易でしょう.

$K := \{a + b\lambda \in \mathbb{C} | a, b \in [0,1]\}$ とすると K は C の中でコンパクト (有界閉集合) で, π が連続ですからその像である $X = \pi(K)$ はコンパクトです.

$\mathbb{C}$ の中の開集合 U を十分小さくとると Λ ずれた値が入らないようにもできます．その範囲内では $\pi|_U : U \to \pi(U) \subseteq X$ は 1 対 1 の対応がつき逆写像も連続である（homeomorphic）ことがわかります．つまり X は局所的には $\mathbb{C}$ の開集合と同じと思えるということです．貼り合わせ部分も問題なくできて，これにより X はコンパクト 1 次元複素多様体になります．

また加算や逆元（マイナス操作）も正則にできることがわかります．

楕円曲線 X 上の関数は $\mathbb{C}$ 上の関数で $f(x+a+b\lambda) = f(x)$, $a, b \in \mathbb{Z}$, $\Lambda = \langle 1, \lambda \rangle$ を満たす関数とみなせます．f を $\mathbb{C}$ 上の二重周期関数と呼んだりします．

m を自然数とし，X 上の m 倍写像 $m : X \ni x \to mx \in X$ を考えると $m(x+y) = mx + my$ なので準同型写像です．$\mathrm{Ker}(m)$ は m 倍して 0 になる点ですが，$\Lambda = \mathbb{Z} + \mathbb{Z}\lambda$ なので

$$\mathrm{Ker}(m) = \left\{ \frac{a}{m} + \frac{b}{m} \in X \;\middle|\; a, b \in \mathbb{Z} \right\} = (\mathbb{Z}/m\mathbb{Z})^2$$

となります．また m は全射です．

4 ペアリング

基本的な用語がだいたい終わったので（ふぅ），漸く本題のペアリングの話に戻れます．

4.1 Weil ペアリングの定義

m を自然数とし，$\mathbb{G}_m$ を $\mathbb{C}$ の乗法群 $\mathbb{C}^* := \mathbb{C} - \{0\}$ とします．X を楕円曲線，$X[m] := \{ x \in X \mid mx = 0 \}$ とします．すると次の完全列を得られます．

$$0 \to X[m] \to X \xrightarrow{m} X \to 0$$

$m : X \to X$ は m 倍写像です．$\mathbb{G}_m$ への Hom を考えることで Ext の完全列を使って次の完全列が得られます．$\mathbb{G}_m$ が乗法群なので行き先は $+$ ではなく $\times$ で表現することに注意．

$$0 \to \mathrm{Hom}(X, \mathbb{G}_m) \to \mathrm{Hom}(X, \mathbb{G}_m) \to \mathrm{Hom}(X[m], \mathbb{G}_m) \to \mathrm{Ext}(X, \mathbb{G}_m) \to \mathrm{Ext}(X, \mathbb{G}_m) \to \mathrm{Ext}(X[m], \mathbb{G}_m)$$

$\mathrm{Hom}(X, \mathbb{G}_m)$ は X から $\mathbb{G}_m$ への正則で準同型の写像全体です．$f \in \mathrm{Hom}(X, \mathbb{G}_m)$ をとると X はコンパクトなので $f(X) \subseteq \mathbb{G}_m$ はコンパクト，つまり $\mathbb{C}$ 内で有界．f は $\mathbb{C}$ 上の周期関数とみなせます．すると $\mathbb{C}$ 上の有界な正則関数は定数しかないので $f = \mathrm{const}$ となります．準同型なので $f(0) = \mathrm{const} = 1$．よって $\mathrm{Hom}(X, \mathbb{G}_m) = \{0\}$ となります．上記長完全列のうち必要な部分を抜き出すと

$$0 \to \mathrm{Hom}(X[m], \mathbb{G}_m) \xrightarrow{\delta} \mathrm{Ext}(X, \mathbb{G}_m) \xrightarrow{m\times} \mathrm{Ext}(X, \mathbb{G}_m)$$

となります．$f \in \mathrm{Hom}(X[m], \mathbb{G}_m)$, $x \in X[m]$ について $1 = f(0) = f(mx) = f(x)^m$．だから $f(x) \in \mu_m = \{ x \in \mathbb{C} \mid x^m = 1 \}$．つまり $\mathrm{Hom}(X[m], \mathbb{G}_m) = \mathrm{Hom}(X[m], \mu_m)$.

$\hat{X} := \mathrm{Ext}(X, \mathbb{G}_m)$ と定義し，これを X の双対楕円曲線と呼ぶことにすると上の列は

$$0 \to \mathrm{Hom}(X[m], \mu_m) \xrightarrow{\delta} \hat{X} \xrightarrow{m\times} \hat{X}$$

となります.

$$\mathrm{Im}(\delta) = \mathrm{Ker}(m\times) = \left\{ x \in \hat{X} \;\middle|\; mx = 0 \right\} = \hat{X}[m]$$

ですから準同型定理により $\mathrm{Hom}(X[m], \mu_m) = \hat{X}[m]$ という同型を得られます.

すると $x \in X[m]$, $f \in \hat{X}[m] = \mathrm{Hom}(X[m], \mu_m)$ にたいしてその値 $f(x) \in \mu_m$ を取るという自然な写像が得られます.

$$e_m : X[m] \times \hat{X}[m] \to \mu_m$$

これを Weil ペアリングと呼びます. X を楕円曲線としましたが, アーベル多様体でも同様に進められます. 作り方をおさらいすればわかるように楕円曲線 X と m 倍写像から基底を使うことなく自然にペアリングを定義できました. これが基底によらない抽象的な定義です.

4.2 Pic^0

さて, $\hat{X}$ の正体に入る前に, またしばらく準備が必要です. まず因子の定義をしましょう.

X を楕円曲線としたとき, X の点の形式的有限和 $D = \sum a_n(P_n)$ を Weil 因子といい, その次数を $\deg D = \sum a_n$ で定義します. X の因子全体の集合を $\mathrm{Div}(X)$ と書きます. 因子の和を

$$D + D' = \sum a_n(P_n) + \sum a'_n(P'_n)$$

とすることで $\mathrm{Div}(X)$ は Abel 群になります.

$$\mathrm{Div}^0(X) = \{\, D \in \mathrm{Div}(X) \mid \deg D = 0 \,\}$$

とすると $\mathrm{Div}^0(X)$ は $\mathrm{Div}(X)$ の部分群です.

順序も入れておきましょう. 2 つの因子 D, D' について $D \geq D'$ であるとは, $D - D' = \sum a_n(P_n)$ について $a_n \geq 0$ for all n とします.

X 上の有理型関数 $f(\neq 0,\ \infty) \in M(X)$ にたいして, $f(z) = 0$ となる z を零点 (zero), $f(z) = \infty$ となる点を極 (pole) といいます. f を z の近傍の局所座標で Laurent 展開して $f(z) = \sum_{i=s}^{\infty} a_i z^i$ となったとき, z が zero なら $s > 0$, z が pole なら $s < 0$ となります. $\mathrm{ord}_z f = s$ と書き, f の z の位数 (order) といいます.

$\mathrm{div}(f) := \sum \mathrm{ord}_P(f)(P)$ と定義すると, f の zero や pole や有限個しかありません. なぜなら無限個あったとすると X はコンパクトなので集積点ができて, 一致の定理からそれは定数関数で 0 か ∞ になってしまうからです. よって $\mathrm{div}(f)$ は X の因子となります.

また f の重複度を込めた zero の数と pole の数は同じで, ある f が定める関数体間 $M(\mathbb{P}^1) \to M(X)$ の拡大次数に等しい) ことが示せて, 結果 $\deg \mathrm{div}(f) = 0$ となります.

2 つの因子 D, D' が線形同値であるとは, ある f があって $D = D' + \mathrm{div}(f)$ となるときにいいます.

f, g を 0 や ∞ でない有理型関数とすると $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$, $\mathrm{div}(f^{-1}) = -\mathrm{div}(f)$ であることは容易にわかります. よって $\mathrm{div} : M(X) \to \mathrm{Div}^0(X)$ は準同型写像になり, $\mathrm{Pic}^0(f) := \mathrm{Div}^0(X)/\sim$ も Abel 群になります. Pic は Picard の略です.

とりあえず, $\mathrm{Pic}^0(X)$ を定義しましたが, これだけでは全然意味がわかりませんね.

4.3 Riemann-Roch の定理

因子がどう大事なのかを見るために少し寄り道します.

天下り的ですがもう少しだけ定義を続けます. 因子 D にたいして $L(D) := \{\, f \mid \mathrm{div}(f) \geq -D \,\} \cup \{0\}$ とします. $L(D)$ はベクトル空間になります. なぜなら 2 つの関数 f, g にたいして $f+g$ は zero は増えることはあっても pole は打ち消し合う可能性しかないからです.

$L(D)$ の次元を $l(D)$ としましょう. $l(D) := \dim_{\mathbb{C}} L(D)$. D と D' が線形同値なとき（すなわちある f にたいして $D = D' + \mathrm{div}(f)$）, $L(D')$ の元に f をかけると $L(D)$ の元になるので $L(D)$ と $L(D')$ はベクトル空間として同型になります.

X 上の正則な関数は定数関数しかなかったので $L(0) = \mathbb{C}$ となります. 一般的に $L(D)$ は有限次元ベクトル空間になるのですが, もっと精密に

定理 4.1. 楕円曲線に対する一番簡単な Riemann-Roch の定理 (の一部): $\deg D > 0$ のとき $l(D) = \deg D$.

が成り立ちます. Riemann-Roch は楕円曲線だけでなく, 1 次元の連結なコンパクトな複素多様体 (=Riemann 面) でも成り立つ定理です.

D が一点 P からなる因子 (P) のとき, $l((P)) = 1$ です. 定数関数は $L((P))$ の元ですので, $L((P))$ は定数関数しかないということです. これは $\mathbb{C}$ 上の二重周期関数で一位の pole を持つものが存在しないことを意味しています.

この定理を使って楕円曲線を射影空間の部分多様体として実現してみましょう.

まず楕円曲線の点 P を固定して $D = n(P)$ という因子を考えてみると, Riemann-Roch の定理から $n > 0$ のとき $l(n(P)) = n$ となります.

$L(2(P))$ は 2 次元で定数関数 1 以外の元 f をとると $L(2(P)) = \langle 1, f \rangle$ となります.

$L(3(P))$ は 3 次元で $L(3(P)) = \langle 1, f, g \rangle$ としましょう. $L(4(P))$ を考えてみます. f は点 P で 2 位の pole だったので f^2 は点 P で 4 位の pole を持ちます. つまり $L(4(P)) = \langle 1, f, g, f^2 \rangle$.

$L(5(P))$ はどうでしょう. 点 P で f が 2 位, g が 3 位の pole を持つので fg は 5 位の pole を持ちます. つまり $L(5(P)) = \langle 1, f, g, f^2, fg \rangle$.

もうひとつ, $L(6(P))$ を考えると f^3, g^2 のどちらも 6 位の pole を持ちます. $\deg L(6(P)) = 6$ ですから, 7 個の基底の候補 $1, f, g, f^2, fg, f^3, g^2$ は線形従属になります.

つまりある $a_1, \ldots, a_7$（全てが 0 ではない）が存在して

$$a_1 + a_2 f + a_3 g + a_4 f^2 + a_5 fg + a_6 f^3 + a_7 g^2 = 0$$

3 次方程式の 2 次の項を消す要領で適当にアフィン変換を施して f と g を取り直すと

$$g^2 = f^3 + af + b \tag{5}$$

と式変形できます. これはいわゆる普通の楕円曲線の定義方程式です.

$\phi : X \ni x \to (f(x) : g(x) : 1) \in \mathbb{P}^2$ としましょう.

実は ϕ は正則で 1 対 1, ϕ の像 $\phi(X)$ は $\mathbb{P}^2$ の中でコンパクトな部分多様体になることが分かります. そうすると 1 次元複素トーラスであった X は式 **??** で定義された多様体と同じものとみなせます.

つまり, 楕円曲線は（f と g を x と y という名前に置き換えると）$y^2 = x^3 + ax + b$ という形しかないということがわかります. 何故, 暗号の入門書などで唐突にこんな方程式が現れ, それしか考えないのかというのは, （1 次元の範囲では）そういうものしかなかったからなのでした.

一般に何かわからない X を調べるとき, X を直接調べるのではなく X 上の関数全体を考えるという方法が

あります. たとえば X がベクトル空間のときは $\mathrm{Hom}_{\mathbb{C}}(X,\mathbb{C})$ は X に同型でした. 楕円曲線のときは正則な関数は定数関数しかなかったので, pole を持ってもよい関数を少しずつ増やすことで, それから作られる $\mathbb{P}^n$ への写像を考えてみたのです. 実は楕円曲線でなくもっと一般のコンパクト Riemann 平面にたいしても同様に $\mathbb{P}^n$ の部分多様体として実現できます.

とりあえず, 因子とそれから作られるベクトル空間に関する次元の定理があるといろいろできるというのが少しは伝わったでしょうか.

4.4 Pic^0 と X

実は楕円曲線 X にたいして $\mathrm{Pic}^0(X)$ は X 自身になることが示せます.

$\deg D = 0$ とします. O を楕円曲線の単位元として, $D+(O)$ という因子を考えると $\deg(D+(O)) = 1$. Riemann-Roch の定理より $l(D+(O)) = 1$. よってある $f \in M(X)$ があって $D' := \mathrm{div}(f) + D + (O) \geq 0$. $\deg D' = 1$ で, 全ての点で 0 以上なので結局 D' は 1 点 P_D からなる因子 (P_D) であることが分かります. すると $D = (P_D) - \mathrm{div}(f) - (O) \sim (P_D) - (O)$.

この P_D は D から一意に定まります. なぜなら $(P)-(O) \sim D \sim (P')-(O)$ とすると $(P) \sim (P')$. つまりある $f \in M(X)$ があって $\mathrm{div}(f) = (P) - (P')$. これは f が P で 1 位の zero, P' で 1 位の pole を持つということです. そうすると $X \ni x \to (f(x):1) \in \mathbb{P}^1$ という写像は全単射正則写像になって X が $\mathbb{P}^1$ になってしまいます. というわけで

$$\phi : \mathrm{Pic}^0(X) \ni D \to P_D \in X$$

という写像を構成できました. $\phi(D+D') = \phi(D) + \phi(D')$ は容易に示せます. P_D はもっと具体的に構成法を示せます.

$P, Q \in X$ とし X 上の点加算として $R = P + Q$ とします. $f(x,y) = ax + by + c$ を P, Q を通る直線の式とすると $f(P) = f(Q) = f(-R) = 0$. よって

$$\mathrm{div}(f) = (P) + (Q) + (-R) - 3(O).$$

$g(x,y) = dx + e$ を R, O を通る直線の式とすると $\mathrm{div}(g) = (R) + (-R) - 2(O)$. よって

$$\mathrm{div}(f/g) = (P) + (Q) - (R) - (O).$$

つまり $((P)-(O)) + ((Q)-(O)) \sim (P+Q) - (O)$.

一般に $D = \sum a_n(P) \in \mathrm{Div}^0(X)$ に対し点加算としての $P_D = \sum a_n P$ をとると $D \sim (P_D) - (O)$ となることがわかります.

さて逆写像は $\phi^{-1}(P) = (P) - (O)$ となります. よって $X \ni P \to (P) - (O) \in \mathrm{Pic}^0(X)$ は同型となります.

4.5 Pic^0 と Ext

$\hat{X}$ の話に戻ります. $T \in X$ を 1 つとったとき, $\tau_T : X \ni P \to P + T \in X$ という T だけ足す関数を考えます. $D = (T) - (O) \in \mathrm{Pic}^0(X) = X$ をとり, $\tau_P^* D = (T-P) - (-P)$ とします.

$\tau_R^* D - D = (T-P) - (-P) - (T) + (O)$ を考えると点の加算として $T - P + P - T = O$ なので Riemann-Roch の定理からある $f_{T,R} \in M(X)$ があって $\tau_R^* D - D = \mathrm{div}(\mathbb{F}_{T,R})$. この f は定数倍を除いて一意です.

$\phi : \mathrm{Pic}^0(X) \to \mathrm{Ext}(X, \mathbb{G}_m)$ を

$$\phi(T)(P,Q) = \frac{f_{T,P}(Q)}{f_{T,P}(O)}$$

で定義します. 定数倍して $f_{T,P}(O) = 1$ としてもよいです. $T = O$ のときは $f_{D,R} = 1$ とします.

$\phi(T)(P,Q)$ が Ext の元であることを確認します.

$$\begin{aligned}\mathrm{div}(f_{T,P+Q}) &= (T-P-Q) - (-P-Q) - (T) + (O) \\ &= (T-P-Q) - (-P-Q) - (T-Q) + (-Q) + (T-Q) - (T) - (-Q) + (O) \\ &= \mathrm{div}(\tau_Q^* f_P) + \mathrm{div}(f_Q)\end{aligned}$$

よって $f_{T,P+Q}(R) = f_{T,P}(R+Q) f_Q(R)$.

$$\frac{\phi(T)(P,Q)}{\phi(T)(P,Q+R)} \cdot \frac{\phi(T)(P+Q,R)}{\phi(T)(Q,R)} = \frac{f_P(Q)}{f_P(O)} \cdot \frac{f_Q(O)}{f_Q(R)} \cdot \frac{f_{P+Q}(R)}{f_{P+Q}(O)} \cdot \frac{f_P(O)}{f_P(Q+R)} = 1.$$

次に単射を確認します. $\mathrm{Pic}^0(X) \ni D$ をとり, $\mathrm{div}(f_{T,P}) = \tau_P^* D - D$ とします. ある $g \in M(X)$ があって

$$\phi(T)(P,Q) = f_{T,P}(Q) = \frac{g(P+Q)}{g(P)g(Q)}$$

とします. $g(0) = 1$ としておきましょう.

$h(Q) := \left(\frac{\tau_P^* g}{g}\right)(Q)$ とすると

$$\begin{aligned}h(Q) &= \frac{g(P+Q)}{g(P)g(Q)} = \phi(T)(P,Q), \\ \tau_P^* D - D &= \tau_P^* \,\mathrm{div}(g) - \mathrm{div}(g).\end{aligned}$$

よって $\tau_P^*(D - \mathrm{div}(g)) = D - \mathrm{div}(g)$.

任意の $P \in X$ について τ_P による引き戻しが変わらないということは $D - \mathrm{div}(g) = 0$. つまり $D = \mathrm{div}(g) \sim 0$ となり単射となりました. 全射も準同型と同様に（出来ると思う... 疲れた...）.

長々とやってましたが, $\hat{X} = \mathrm{Ext}(X, \mathbb{G}_m)$ と $\mathrm{Pic}^0(X)$ と X が同一視できることにより, Weil ペアリングが

$$e_m : X[m] \times X[m] \to \mu_m$$

となりました.