類体論、特に一般相互法則の証明について

早稲田大学　理工学部　足立恒雄

序　類体論は、仏像で譬えれば、高木［11］によって像が作られ、アルチン［１］の手によって開眼された。アルチンの一般相互法則は正に「類体論の画竜点睛」（高木の言葉）というわけである。ハーセの報文［５］は、簡易化されてはいるが、本質的には高木の仕事とアルチンの仕事を歴史的な順序で忠実に叙述したものである（Ｉ，Ｉａが書かれた段階では相互法則はまだ日の目を見ていなかったのだからこれは当然である）。すなわち、まず高木の基本等式を導き、それを元に存在定理を証明し、その後分解定理、同型定理などの証明に向かう。次にそれらの成果を踏まえて一般相互法則が証明されるのである。以後、数多くの人達によって類体論の証明の簡易化と整備が図られてきたが、高木自身の手による著書［12］まで含めて（高木はその中で、「多少躊躇の後、．．．直観性を犠牲にして、相互律の直接証明法を述べることにした」と記している）すべて、一直線に相互法則の証明を目指し、その系として分解定理などを導き、最後に存在定理の証明に向かう形式を取っている。また、ハーセ、シュヴァレー等による局所類体論の確立以後、局所類体論も同時並行的に扱い、局所体の理論を類体論の証明に援用するのが一般的になった。

類体論を主題にした書物・論文としては、シュヴァレー［３］、高木［12］、アルチン＝テイト［２］、ヴェイユ［14］、テイト［13］、河田［９］、彌永［８］、ノイキルヒ［10］などが挙げられる。この中で、シュヴァレーの論文における相互法則の証明法は、アルチンが用いた円分体交差法を二重に適用して円分体の場合に帰着するもので、今まで知られている最も簡潔な証明と思われる。しかし、高木［12］を引用すると、「証明の方法は巧妙ではあるが、それは高度に技術的で、直観性がまったく没却されている」。一言で言えば、高度にsophisticated であるということだろう。では、その後の諸家の証明が直観的で、分かりいいかというと、一概にそうは言えないように思う。中でも最も公理主義的な方法（類構造の概念）を一貫して採用した河田［９］についてそのことを見てみると、整然としていて、しかも簡潔ではあるが、数論的意味のいま一つはっきりしないコホモロジー論の予備知識がかなり必要となり、本質の直観的理解を妨げている趣がある。

例えば、ガロア群からイデール類群への写像が先に与えられ、その逆写像としてシュヴ

ァレー写像（ノルム剰余写像）が定義されるという点は問題点の一つのように思われる。イデアルに対するアルチン＝ハーセ写像は本来単純明解な意味を持つ。それが、最後に至って定義が与えられるというのは不自然と言わねばならない。この事情はテイト［13］、彌永［８］、ノイキルヒ［10］でも同様である。なお、ヴェイユ［14］では群指標の概念を用いてシュヴァレー写像が定義されるから、写像が逆向きというわけではないが、直観的で素朴とは言い難い。

次にいわゆる高木の第１不等式（第２不等式とも呼ばれる）の算術的証明について考えてみよう。高木はＬ関数による簡明な証明を与えた。しかし算術における命題を解析的に証明するのは一つの欠陥であるとみなされて、算術的な証明が求められた。シュヴァレー［４］はその期待に応えたものであったが、決して簡単な証明とは言えないし、この方法では算術級数の素数定理の一般化は得られない。その後はこの証明を採用するのが一般的になっていったけれども、類体論とＬ関数との関連は単なる技術的なものではないことはアルチンのＬ関数に関する業績を待つまでもなく自明なことである。例えば、ノイキルヒ［10］のように類体論の証明が終わった後にＬ関数に関する記述を入れるのならば、最初から解析的な証明を採用した方が簡潔で良いと思われる。

最後に、イデアルとイデールの関係について触れておこう。因子論的方法とイデアル論的方法とはその成立史上の問題が絡み合って、数論における対立的な方法とみなされてきた（例えば、ハーセ［６］、［７］参照）が、どちらかといえば、因子論の方がイデール論となじみ易い概念であることは明らかである。本論文では、イデアルという用語を用いたが、これを因子（divisor)という用語に読み替える方が、イデールも登場する関係上、違和感が少ないかもしれない。

本論文では、アルチンの原論文が結局は一番簡単で、予備知識も少なくて済むという考えに基づいて、一般相互法則の証明をより直観的に納得し易い形に再構成することを目的としたものである。アルチンの証明は分解定理、存在定理など高木の類体論を利用している。しかしよく見てみると、そこで用いられる存在定理と、分解定理の証明に用いられる存在定理とは限定された種類のものであるから、それだけは先に、簡単に証明を与えることが可能である。完全な存在定理は、現行の諸本同様相互法則の後に回せば、高木の原論文よりは見通しの良い証明を与えることができる。というわけで、アルチンの原論文の方法に立ち戻って証明を構成するという方法は、いきなり頂上を目指すのではなく、いくつかのキャンプを経て登頂するのに似てeasy goingなように思われる。

§1　高木の類体論　kを有限次代数体とする。J_k をkのイデール群、C_k をイデール類群、すなわち$C_k = J_k / k$とする。K／kを有限次代数体とするとき、$N_{K/k}$ でもってKからkへのイデール、ないしイデール類群のノルム写像を表すことにする。このとき

定理1（高木の第1不等式）　任意のガロア拡大K／kに対して、不等式

$$(C_k : N_{K/k} C_K) \leqq [K : k] \qquad (1)$$

が成り立つ。同じことだが、コホモロジーの用語で言えば、

$$|H^0(G, C_K)| \leqq [K : k]$$

となる：ここにGはK／kのガロア群を表す。

定理1の証明は対応するイデアル群に関する命題を解析的な手段で行うのが一番簡単であることは序でも述べたが、副産物もある。まずmをkの因子とし、I_m、$I_{m,K}$をそれぞれk、Kのmと素な分数イデアルのなす群、S_m をmを法とするStrahlとする：

$$S_m = \{(\alpha) \mid \alpha \in k,\ \alpha \equiv 1 \pmod{m}\}$$

このとき、定理1は

$$(I_m : S_m N_{K/k} I_{m,K}) \leqq [K : k]$$

と書き換えられるのだが、さらに：

定理1の系　K／kをガロア拡大とする。kの因子mに対して$H_m = S_m N_{K/k} I_{m,K}$と置けば、$I_m / H_m$ の各類には絶対1次の素イデアルが無数に存在する。

これは高木の第1不等式の証明から直ちに知られることである（例えば、高木［12］p. 171 参照）。類体の定義は、このとき次で与えられる：

類体の定義　（1）において等号が成り立つとき、ガロア拡大K／kは$N_{K/k} C_K$（また$S_m N_{K/k} I_{m,K}$）の類体であるという。

簡単な解析的考察によって次のことが分かる：

定理2　ガロア拡大K／kが$H_m = S_m N_{K/k} I_{m,K}$の類体であるためには、$H_m$ に属す

る素イデアルがほとんどすべてK／kにおいて完全分解することが必要十分である。

定理２の系（類体の結合定理）　K_1／k，K_2／kがそれぞれH_1，H_2（どちらもmを法とする）の類体ならば、K_1K_2／kは$H_1 \cap H_2$の類体である。

系の証明は定理２と類体の定義から容易である。類体の一意性定理、順序定理などはこの系から直ちに分かる。高木はK／kがアーベル拡大であれば常に、定理１において逆の不等式が成り立つことを証明した。すなわち、

定理３（高木の第２不等式）　K／kが特にアーベル拡大であれば、不等式

$$(C_K : N_{K/k}\, C_K) \geqq [K : k]$$

が成り立つ。したがって定理１と合わせて、特に等号が成り立つ（高木の基本不等式）、すなわち、アーベル拡大は常に対応するノルム群$N_{K/k}\, C_K$の類体である。イデアル群で言い換えると、K／kがアーベル拡大のときは、適当な法mを取ると、

$$(I_m : H_m) \geqq [K : k]$$

が成り立つ。mとしてはK／kで分岐する素点のノルム剰余の臨界冪の積を取れば十分であるが、その倍数であるような因子はすべてこの役割を果たす。

等号が成り立つということは、コホモロジー群で言えば

$$|H^0(G, C_K)| = [K : k]$$

となることを意味する。

定理２、定理３から次の命題が容易に導かれる：

定理４（類体の推進定理）　アーベル拡大K／kがイデアル群H_mの類体なるとき、Mをk上の任意の代数体とすれば、KM／MはMにおけるイデアル群Hの類体である。ただし$H = \{A\ (\in I_{m,K}) \mid N_{M/K}\, A \in H_m\}$とする。

円分体論は類体論の雛形であるというにとどまらず、その証明において本質的な役割を果たす。中でも次は相互法則の証明に用いられるが、証明は有理数体上の円分体論を定理４を用いてk上に持ち上げればよい：

定理４の系（円分体における一般相互法則）　イデアル群H_mの類体Ｚ／ｋが特に円分体（すなわち、１の冪根をｋに添加して得られる体の部分体）であるとする。このとき、アルチン＝ハーセ写像$\underline{a} \to (\underline{a}, Z/k)$は同型対応：$I_m/H_m \longrightarrow Gal(Z/k)$を与える：したがって、特に、$\underline{a} \in H_m \Leftrightarrow (\underline{a}, Z/k) = 1$である。

以上において本質的に難しいのは定理３（高木の第２不等式）だけである。高木は素数次の巡回拡大の場合に帰着し、今でいうコホモロジー群の計算を行ってこれを証明した。その後、エルブラン商の考え方が導入されて、一般の巡回拡大の場合に第２不等式を直接証明できるようになった。すなわち、Ｋ／ｋが巡回拡大である場合、

$$q(C_K) = |H^0(G, C_K)| / |H^1(G, C_K)|$$

と置くとき（エルブラン商）、

$$q(C_K) = [K : k] \qquad (2)$$

が示されるのである。エルブランの貢献によっても、なお証明は嫌気がさすようなものであったが、さらに、イデールを用いるご利益によって、各素点ｐに対して$|H^0(G^p, K^{p\times})| = [K^p : k_p]$を証明することに還元できることが分かり、定理３の証明も大いに簡易化された：現在では一般的になったこの証明法はシュヴァレー［４］によるものである。（２）と高木の第１不等式によって巡回拡大に対しては基本等式が成り立つことと同時に、

$$|H^1(G, C_K)| = 1$$

という重要な結果が併せて得られるが、これは、シロー群への制限と群の位数に関する数学的帰納法を用いて容易に一般のガロア拡大の場合に拡張される（一般相互法則の証明のためだけなら、巡回拡大の場合だけで良いが、見場の関係で一般化しておく）：

定理５　任意のガロア拡大Ｋ／ｋに対して

$$|H^1(G, C_K)| = 1$$

および

$$|H^2(G, C_K)| \leqq [K : k]$$

が成り立つ。

§２　同型定理、分解定理　簡単のため、今後はｉ＝0、1、2 に対してＨ^{i}（Ｇ，Ｃ$_{K}$）をＨ^{i}（Ｋ／ｋ）と略記する。｛Ｃ$_{K}$|Ｋ／ｋは有限次代数体｝は類構造（class formation）を持つことが、以下のように簡単に証明される：

定理６　任意のガロア拡大Ｋ／ｋに対して

$$H^{2}(K/k) \simeq Z/nZ$$

が成り立つ：ここにｎ＝［Ｋ：ｋ］とする。

証明　ｎ次の巡回円分拡大Ｚ／ｋを取る。こういうＺは無数にあるから、簡単のため、Ｚ∩Ｋ＝ｋとしてもよい。Ｈ^{1}（ＫＺ／Ｚ）＝Ｈ^{1}(ＫＺ／Ｋ）＝０であるから、次の二つの完全系列が得られる：

$$0 \longrightarrow H^{2}(K/k) \xrightarrow{Inf^{(1)}} H^{2}(KZ/k) \xrightarrow{Res^{(1)}} H^{2}(KZ/K)$$

$$0 \longrightarrow H^{2}(Z/k) \xrightarrow{Inf^{(2)}} H^{2}(KZ/k) \xrightarrow{Res^{(2)}} H^{2}(KZ/Z)$$

定理４の系により、Ｈ^{2}（Ｚ／ｋ）≃Ｈ^{0}(Ｚ／ｋ）はGal(Ｚ／ｋ）≃Ｚ／ｎＺに同型である。そこでその生成元を一つ取って$\xi_{z/k}$とする。しからばRes$^{(1)}$ Inf$^{(2)}$（$\xi_{z/k}$）＝０が成り立つ。なぜならＺ／ｋ，ＫＺ／Ｋはいずれも巡回拡大であるから、Ｈ^{2}≃Ｈ^{0}である。そこで

$$H^{0}(Z/k) \xrightarrow{\sim} H^{2}(Z/k) \xrightarrow{Inf^{(2)}} H^{2}(KZ/k) \xrightarrow{Res^{(1)}} H^{2}(KZ/K) \xrightarrow{\sim} H^{0}(KZ/K)$$

という写像をたどってみると、これは$\underline{a}$ mod $N_{z/k}$ Ｃ$_{z}$に$\underline{a}$ mod $N_{Kz/K}C_{Kz}$を対応させる写像であることが分かる。しかるに（$\underline{a}$，ＫＺ／Ｋ）＝（$N_{K/k}\underline{a}$，Ｚ／ｋ）＝（$\underline{a}^{n}$，Ｚ／ｋ）＝１である。そこで、円分体ＫＺ／Ｋに定理４の系が適用できてａ∈$N_{Kz/K}C_{Kz}$が得られるからである。故に、Inf$^{(1)}\eta$＝Inf$^{(2)}$（$\xi_{z/k}$）を満たすη∈Ｈ^{2}（Ｋ／ｋ）が存在する。これはηの位数がｎであることを示しているが、定理５により|Ｈ^{2}(Ｋ／ｋ)|≦ｎであるので、定理の主張が示されたことになる。□

定理６の系１（同型定理）　Ｋ／ｋをアーベル拡大とすると、

$$H^{0}(K/k) \simeq Gal(K/k)$$

証明　K／kが巡回拡大である場合は、定理５によってH^0（K／k）$\simeq H^2$（K／k）$\simeq$Gal(K／k）が成り立つ。一般のアーベル拡大の場合は類体の結合定理（定理２の系）によって巡回拡大の場合から導かれる。□

定理６の系２（限定された存在定理）K／kをアーベル拡大とし、Hを$C_k \supset H \supset N_{K/k}\, C_K$なる群とする。このとき、$H = N_{M/k}\, C_M$を満たすK／kの中間体Mが存在する。

証明　類体の一意性により、K／kの部分体の集合｛M／k｝とノルム群の集合｛$N_{M/k}\, C_M$｝とは１対１に対応する。一方、系１によって$C_k / N_{K/k}\, C_K \simeq$Gal(K／k）が成り立つから、$C_k$と$N_{K/k}\, C_K$との間には、Gal(K／k）の部分群と同じだけしか部分群が存在しない。□

H^0（K／k）とGal(K／k）との同型対応がアルチン＝ハーセ写像（＊、K／k）によって具体的かつfunctorialに与えられるというのが一般相互法則の主張である。以降、相互法則の証明のための準備をする：

補題１　自然数a＞１とnとが与えられているとき、次のような素数ℓが無数に存在する：あるtに関してaは$(Z/\ell^t Z)^\times$においてnの倍数を位数として持つ。

証明（高木［12］p.209による）　円のn等分多項式をF（x）とし、ℓをF（a）の素因数とすると、$a^n - 1$はℓで割り切れるので、これがちょうどℓ^tで割り切れるとすれば、$(Z/\ell^t Z)^\times$におけるaの位数はnである：もしも仮にその位数fがnより小さいとすれば、fはnの約数で、

$$x^n - 1 = (x^f - 1)\, F(x)\, G(x)$$

においてG（x）は整数係数の多項式である。したがって$(a^f - 1)\, F(a)$は$a^n - 1$を割り切る。$a^f - 1$がℓ^tで割り切れるとすると、これはtの取り方に矛盾する。

次にq＞ℓなる素数qを取って、nにqnを代用すれば、aの$(Z/\ell_1^{\,t} Z)^\times$における位数がqnなる素数$\ell_1$がある。$\ell_1 \geqq q > \ell$であるから、結局問題に適する素数$\ell$が無数にあることになる。□

補題２　Ｋ／ｋは巡回拡大で、イデアル群$H_{\mathfrak{m}}$の類体であるとする。また$\mathfrak{p}$は$\mathfrak{m}$と素なｋの素イデアルで、Ｋ／ｋでは完全分解しないとする。このとき、

①　$\mathfrak{p}\in Spl(M/k)$、すなわち$\mathfrak{p}$はＭ／ｋで完全分解、

②　ＫＭ／Ｍは円分拡大

なる性質を満たすＭ／ｋ（$K\subsetneq M$）が存在する。

証明　$n=[K:k]$とし、$N_k\,\mathfrak{p}=p^f$を$\mathfrak{p}$の絶対ノルムとする。補題１のｎとしてｎｆ、ａとしてｐを取り、そこで保証されるℓ^tに対して、円のℓ^t分体をＦとする。簡単のため、$F\cap K=\mathbb{Q}$であるようにしておく。Ｆ／$\mathbb{Q}$は巡回拡大で、（ｐ）は不分岐、しかもその次数はｎｆの倍数である。したがって$\mathfrak{p}$のＦｋ／ｋにおける相対次数をn_0とすれば、n_0はｎの倍数である。そこで、Ｆｋ／ｋならびににFK/kにおける$\mathfrak{p}$の分解体をそれぞれM_0，Ｍと記すことにすると、$M\cap Fk=M_0$が成り立つ。$\mathfrak{p}$がFK/kで不分岐であることと$n\mid n_0$によって、$Gal(FK/M)$は位数n_0の巡回群であることが知られる。これは$[FK:M]=[Fk:M_0]$を意味するので、$FK=FM$が結論される。①はＭの定義から明らかである。Ｆｋ／ｋが円分的だから、ＦＭ／Ｍ、したがってＫＭ／Ｍも円分的になるから②も成り立つ。なお$\mathfrak{p}\notin Spl(K/k)$によって$K\subsetneq M$となる。□

命題１　Ｋ／ｋをイデアル群$H_{\mathfrak{m}}$の類体とする。ｍと素なｋの素イデアル$\mathfrak{p}$に対して、

$$\mathfrak{p}\in H_{\mathfrak{m}}\iff \mathfrak{p}\in Spl(K/k)$$

が成り立つ：$Spl(K/k)$はＫ／ｋで完全分解するｋの素イデアルの集合を表す。

証明　⇐は明らかである。⇒を示すためには、類体の結合定理によって、Ｋ／ｋは巡回拡大であるとしてよい。そこで、Ｋ／ｋは巡回拡大として、$\mathfrak{p}\notin Spl(K/k)$と仮定する。$\mathfrak{p}$に対し、補題２を満たす拡大Ｍ／ｋを取る。$\mathfrak{p}$はＭ／ｋで完全分解するから、$\mathfrak{P}$を$\mathfrak{p}$のＭにおける素因子とすれば$\mathfrak{p}=N_{M/k}\,\mathfrak{P}$。仮に$\mathfrak{p}\in H_{\mathfrak{m}}$とすれば、類体の推進定理により、$\mathfrak{P}$が円分体ＫＭ／Ｍに対応するイデアル群に属することになり、$(\mathfrak{p},\ K/k)=(\mathfrak{P},\ KM/M)=1$を得る。これは$\mathfrak{p}\notin Spl(K/k)$に矛盾する。故に$\mathfrak{p}\notin H_{\mathfrak{m}}$となるから、⇒が示せた。□

$H_{\mathfrak{m}}$に属するほとんどすべての素イデアルはＫ／ｋで完全分解することはすでに分かっ

ている（定理２）のだが、この命題はそのことに例外のないことを示している。この拡張として次が成り立つ：

定理７（分解定理）　アーベル拡大Ｋ／ｋはイデアル群H_mの類体であるとする。このとき、$\underline{m}$と素なｋの素イデアル$\underline{p}$のＫ／ｋにおける相対次数は$\underline{p}$のI_m/H_mにおける位数に一致する。

証明　Ｚ／ｋを$\underline{p}$のＫ／ｋにおける分解体とする。Ｚに対応するｋのイデアル群をH_zとすると$H_z \supset H_m$。一方Ｚにおいて$\underline{p}$が完全分解することによって$\underline{p} \in H_z$が成り立つ。そこで$C = \underline{p} H_m$と置く。Ｃで生成されるI_m/H_mの部分群をH'/H_mとすると$H_z \supset H'$である。定理６の系２によりH'の類体K'/kが存在する。$H_z \supset H'$であるからＫ′⊃Ｚが成り立つが、命題１により$\underline{p} \in Spl(K'/k)$なので、Ｚが$\underline{p}$の分解体であることと合わせて、Ｋ′⊂Ｚも成り立つ。したがってＫ′＝Ｚ、すなわち$H' = H_z$。これは（Ｋ：Ｚ）＝（H_z：H_m）が$\underline{p} H_m$の位数に等しいことを意味する。□

命題２　Ｓを奇素数の有限集合とし、ｑをｑ∉Ｓなる奇素数とする。またｍ（＞１）を任意に与えられた整数とする。このときつぎのような性質を持つｍ次巡回体Ｆ／Ｑが無数に存在する：

（ｉ）　ｑはＦ／Ｑで惰性する；すなわち（ｑ，Ｆ／Ｑ）は$Gal(F/\mathbb{Q})$を生成する、

（ii）　$(\forall p \in S)\ p \in Spl(F/\mathbb{Q})$

命題２の系　任意に与えられた素数の組$p_1,\ldots,p_t$と、同じく任意に与えられた自然数の組$n_1,\ldots,n_t$に対して、次の性質を持つアーベル拡大Ｆ／Ｑが無数に存在する：

(i)　各p_iのＦ／Ｑにおける分解体をF_iとすると、$Gal(F/\mathbb{Q})$は$Gal(F/F_1),\ldots, Gal(F/F_t)$の直積である。

(ii)　$[F : F_i] = n_i$　$(i=1,\ldots,t)$。

(iii)　$p_1,\ldots, p_t$はＦ／Ｑで分岐しない。

「命題２⇒系」の証明　$S = \{p_1, \ldots, p_t\} - \{p_i\}$、$q = p_i$、$m = n_i$として命題２を適用して得られる体を$M_i$とし、合併体$\bigcup_i M_i$をＦ、合併体$\bigcup_{j \neq i} M_j$を$F_i$と記

す。このF, F_i $(i=1,\ldots,t)$ が条件を満足することは容易に見てとれる。□

命題2の証明を与えよう。この証明はアルチン［1］による。命題2は有理数体上のアーベル拡大の話であるから、既約剰余類群の言葉で表すことができる、すなわち：

命題2′ m (>1) を与えられた整数とし、p, p_1, ・・・, p_t を相異なる奇素数とするとき、次の性質を持つような素数ℓを取ることができる；

$A=(\mathbb{Z}/\ell\mathbb{Z})^\times$, $H=A^m$ と置くと、

(i)　pHはm次巡回群A/Hの生成元である、

(ii)　$p_i \in H$ $(i=1,2,\ldots,t)$

証明　$\ell \equiv 1 \pmod m$ を満たす素数ℓを選び、$k_m=\mathbb{Q}(\zeta_m)$ と置く；ここにζ_mは1の原始m乗根である。$\underline{\ell}$をℓのk_mにおける素因子の一つとすれば、$\ell \in Spl(k_m/\mathbb{Q})$によって法$\underline{\ell}$の剰余類の各類は有理整数を代表に選ぶことができる。したがって特に、m冪剰余のなす群はHと一致する。そこで、aをmと素な整数とすると、aHの位数は$\sigma=(\underline{\ell}, k_m(\sqrt[m]{a})/k_m)$の位数と一致する；これは$\sigma^i=1 \Leftrightarrow a^{i(\ell-1)/m}\equiv 1 \pmod \ell$から簡単に分かることである。故に、(i), (ii)を満たすためには

(i)′　$(\underline{\ell}, k_m(\sqrt[m]{p})/k_m)$の位数は$m$である、

(ii)′　$(\underline{\ell}, k_m(\sqrt[m]{p_i})/k_m)=1$　$(i=1,2,\ldots,t)$

が成り立つように$\underline{\ell}$を取ればよい。$k_m(\sqrt[m]{p})/k_m$がH_1の類体、$L=k_m(\sqrt[m]{p_1}, \ldots, \sqrt[m]{p_t})$は$k_m$上$H_2$の類体であるとする；$H_1, H_2$は共通の法$\underline{m}$によって定義されるようにしておく。定理7によって(i)′、(ii)′は

(i)″　$\underline{\ell}H_1$の位数はmである、

(ii)″　$\underline{\ell} \in H_2$

と言い換えられる。pはmを割らない奇素数なので$[k_m(\sqrt[m]{p}) : k_m]=m$が成り立つから、$\underline{a}H_1$の位数が$m$なるイデアル$\underline{a}$が存在する（同型定理による）。また、分岐の状況を調べてみれば$k_m(\sqrt[m]{p})\cap L=k$であるから、$H_1 H_2 = I_m$が成り立つので、$(\underline{a}H_1/S_m)\cap(H_2/S_m)\neq\phi$を得る。左辺の類から絶対1次の素イデアル$\underline{\ell}$を取れば（定理1の系）、$N_k \underline{\ell}=\ell\equiv 1 \pmod m$が成り立ち、(i)″, (ii)″が満たされる。□

§３　一般相互法則　この節では次の定理の証明を与える：

定理８（一般相互法則）　Ｋ／ｋがアーベル拡大の場合、シュヴァレー写像$\underline{a} \longrightarrow (\underline{a}, K/k)$から同型写像：$C_K / N_{K/k}\, C_K \longrightarrow Gal(K/k)$が誘導される。

イデアル群で同じことを表現すると、

定理８′　Ｋ／ｋが$H_m = S_m\, N_{K/k}\, I_{m,K}$の類体であるとき、アルチン＝ハーセ写像$\underline{a} \to (\underline{a}, K/k)$から同型写像：$I_m / H_m \longrightarrow Gal(K/k)$が誘導される。

ここに、アルチン＝ハーセ写像とは素イデアルに対して定義されるアルチン写像から積によって一般のイデアルに拡張された写像のことである。シュヴァレー写像もアルチン＝ハーセ写像も同一の記号を用いるが、混同が起こることはないであろう。さて、定理の証明がＫ／ｋが巡回拡大の場合に還元されることは類体の順序定理から直ちに分かる。またアルチン＝ハーセ写像が全射であることも次のようにして容易に分かる。すなわち、ｎ次巡回拡大Ｋ／ｋに対して、ＫＭ／Ｍが円分拡大で、しかもＫ∩Ｍ＝ｋであるようなｎ次巡回拡大Ｍ／ｋを取る。右のダイアグラムは可換であるから、

$$\begin{array}{ccc} I_{m,M} & \xrightarrow{(*,\,KM/M)} & Gal(KM/M) \\ \downarrow{\scriptstyle N_{M/k}} & & \downarrow{\scriptstyle \wr\ Res} \\ I_m & \xrightarrow{(*,\,K/k)} & Gal(K/k) \end{array}$$

上の写像の全射性から下の写像の全射性が従う。したがって、高木の基本等式によって、

$$\underline{a} \in H_m \Longrightarrow (\underline{a}, K/k) = 1 \qquad (3)$$

を示せば十分である。

ここで証明の基本的な考え方を述べておこう。ｋのイデアル$\underline{a}$に対して、次のような拡大Ｍ／ｋが存在するとせよ：

①　$\underline{a} = N_{M/k}\, \underline{A}$と表せる、

②　ＫＭ／Ｍは円分拡大である。

そこで、$\underline{H} = \{\underline{A}\ (\in I_{m,M}) \mid N_{M/k}\, \underline{A} \in H_m\}$と置くと、推進定理によってＫＭ／Ｍは$\underline{H}$の類体である。故に、円分体の相互法則によって、$\underline{a} \in H_m \Rightarrow \underline{A} \in \underline{H} \Rightarrow (\underline{a}, K/k) = (\underline{A}, KM/M) = 1$である。これによって、$\underline{a}$に対して①、②を満足するような

拡大体M／kが存在することがいえれば相互法則は一般的に成り立つことになる。任意の$\underline{a}$に対してこれを証明することはできない（あるいは容易でない）が、いくつか仮定を置けば示すことができる。すなわち、

命題３　K／kは巡回拡大で、イデアル群H_mの類体であるとする：ただし$\underline{m}$は２の素因子をすべて含むように取っておく。またSは$\underline{m}$と素なkの素イデアルの有限集合で、次の２条件を満足するものとする；

(i)　Sの素イデアルはそれぞれ異なる有理素数の上にある：すなわち、$\underline{p}$，$\underline{q}$を相異なるSの素イデアルとし、p，qをそれぞれ$\underline{p}$，$\underline{q}$が割り切る有理素数とすればp≠qである。

(ii)　$(\forall \underline{p} \in S)\ \underline{p} \notin Spl(K/k)$。

このとき、

①　$(\forall \underline{p} \in S)\ \underline{p} \in Spl(M/k)$、

②　KM／Mは円分拡大

なる性質を持つ拡大M／kが存在する。

命題３の系　K／k、H_mに関しては命題３と同じとする。またkのイデアル$\underline{a}$の素因子の集合をSとする。Sが命題３の仮定(i),(ii)を満たすならば、（３）が成り立つ。

これは命題３に先行する考察から明らかである。命題３において、Sがただ一つの素イデアル$\underline{p}$からなる場合はすでに証明してある（§２、補題２）。一般の場合の証明は補題１の代わりに補題３を用いるというだけのことである：

命題３の証明　$S=\{\underline{p}_1,\ldots,\underline{p}_t\}$とし、$N_k\underline{p}_i=p_i^{f_i}$を$\underline{p}_i$の体kからの絶対ノルムとする。Fを素数の組$p_1,\ldots,p_t$と、自然数の組$n_1=nf_1,\ldots,n_t=nf_t$（ここにn＝［K：k］）に対して命題２の系（§２）で保証された体Fのうち$F\cap K=\mathbb{Q}$なるものを取る。

Fk／kにおける$\underline{p}_i$の分解体をF_iとすると、Fk／F_iはn次の巡回拡大である。なぜなら、$\underline{p}_i$のFk／kにおける分解群は（$\underline{p}_i$,Fk／k）の位数が（$p_i^{f_i}$,F／$\mathbb{Q}$）の位数に等しいことによって、位数nの巡回群となるからである。$M_0=\bigcap_{\downarrow} F_i$と置くときGal(Fk／$M_0$)は（n,...,n）型である。なぜならGal(Fk／M_0)は（$\underline{p}_i$，Fk／

k）で生成されるが、制限によって得られる写像Gal(Fk／M_0)→Gal(F／Q) は単射であって、Gal(F／Q) は（p_i,F／Q）(i=1,...,t) の直積だからである。

次にFK／kにおける$\underline{p}_i$ の分解体をZ_i とすると、FK／Z_i もn次の巡回拡大である。なぜなら、$\underline{p}_i$ のK／kにおける分解群は位数がnの約数の巡回群だからである。そこで$M=\bigcap_i Z_i$ と置くと、明らかに$M\cap Fk=M_0$ であるが、さらに Gal(FK／M) も（n,..., n）型であることがわかる。なぜなら、制限によって得られる写像Gal(FK／M) →Gal(Fk／k) を考えると、$\sigma_i=(\underline{p}_i, FK/k)$ の像は（$\underline{p}_i$, Fk／k）で、これらはGal(Fk／M_0)の独立な生成系をなす。故に、$n^t \geqq \#\{\sigma_1,...,\sigma_t\}_{gen} \geqq [Fk:M_0]=n^t$ となり、Gal(FK／M) ≃Gal(Fk／M_0)が得られるからである。このことから同時に、FK＝FMも得られる。

このMが求める体であることを示そう。まず$\underline{p}_i \in Spl(M/k)$ はMの定義から明らかである。つぎに、Fk／kが円分的であるから、FM／Mも円分的、したがってその部分体であるKM／Mも円分的であることになる。□

最後に、一般に（3）が成り立つことを証明しよう：ただし、K／kは先に述べたように巡回拡大とし、$\underline{m}$は2の素因子をすべて含むとする。

$\underline{a}=\underline{p}_1^{n_1}\cdots\underline{p}_t^{n_t}$ を$\underline{a}$の素イデアル分解とする。今$\underline{p}_1$ と$\underline{p}_2$ が同じ素数の上にあるとしよう。$p_1,...,p_t$ とは異なる素数の上にあり、$\underline{q}_2 \equiv \underline{p}_2 \pmod{H_m}$ を満たすような素イデアル$\underline{q}_2$ を取る：これは§1の定理1の系によって可能である。$\underline{b}=\underline{p}_1^{n_1}\underline{q}_2^{n_2}\cdots\underline{p}_t^{n_t}$(すなわち、$\underline{b}$は$\underline{a}$の$\underline{p}_2$ を$\underline{q}_2$ に置き換えたもの）と置くとき、$\underline{a}\underline{b}^{-1}=(\underline{p}_2\underline{q}_2^{-1})^{n_2}\in H_m$ であるから、（$\underline{a}\underline{b}^{-1}$, K／k）＝1を得る。実際、$p_2$, $\underline{q}_2$ $\in Spl(K/k)$なら、このことは明らかであるし、$\underline{p}_2$, $\underline{q}_2$ $\notin Spl(K/k)$の場合は、命題3の系によって（$\underline{p}_2\underline{q}_2^{-1}$, K／k）＝1を得るからである。故に、$\underline{b}$が（3）を満たすこととと$\underline{a}$が（3）を満たすことは同値である。この操作を繰り返して、$\underline{a}$の素因子はいずれも相異なる素数の上にあるとして証明すればよいことが分かる。次に、例えば$\underline{p}_1 \in Spl(K/k)$ とする。このときは、$\underline{b}=\underline{p}_2^{n_2}\cdots\underline{p}_t^{n_t}$と置くと、$\underline{a}\underline{b}^{-1}=\underline{p}_1^{n_1}\in H_m$ であるから、§2の命題1によって（$\underline{a}\underline{b}^{-1}$, K／k）＝1。故に、$\underline{a}$が（3）を満たすことは$\underline{b}$が（3）を満たすことと同値である。以上によって、$\underline{a}$の素因子の集合Sは命題3の条件(i),(ii)を満足しているとして良い。従って命題3の系によって、一般的に（3）が証明された。□

文献

[1] Artin, E., Beweis des allgemeinen Reziprözitatsgesetzes. Abh. Math. Sem. Univ. Hamburg, 7(1927), 46-51

[2] Artin-Tate, Class Field Theory, Harvard, 1961

[3] Chevalley, C., Sur la théorie du corps de classes dans le corps finis et les corps locaux. J. Fac. Sci. Tokyo Univ. 2 (1933), 365-476

[4] ———— , La théorie du corps de classes, Ann. of Math. 41 (1940), 394-417

[5] Hasse, H., Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper I, Ia, II. Jber. dt. Mat. Verein. 35 (1926), 1- 55;36(1927), 233-311; Exg. Bd. 6(1930), 1-204

[6] ——— , Zahlentheorie, Berlin, 1949

[7] ——— , Kurt Hensel zum Gedächtnis, Crelle's Jour. 187(1950), 1-13

[8] 彌永昌吉編、数論、岩波書店、1969

[9] 河田敬義、代数的整数論、 共立出版、1957

[10] Neukirch, J., Class Field Theory, Berlin, 1980

[11] Takagi, T., Über eine Theorie des relativ-Abel'schen Zahlkörpers. J. Coll. Sci. imp. Univ. Tokyo, 41(1920), Nr. 9, 1-133

[12] 高木貞治、 代数的整数論、岩波書店、1949

[13] Tate, J., Global Class Field Theory, in "Algebraic Number Theory" ed. by Cassels-Fröhlich, Academic Press, 1967

[14] Weil, A., Basic Number Theory, Berlin, 1967