İstanbul Üniv. Fen Fak. Mat. Der., 53 (1994), 3-4

THE DECOMPOSITION OF THE PRIME IDEALS FOR SOME PARTICULAR FIELD EXTENSIONS

Ion ARMEANU

University of Bucharest, Physics Faculty, Mathematics Dept.,
Bucharest-Magurele, P.O. Box MG-11, ROMANIA

Summary : In this note we prove that for a normal field extension $K \subset L$ whose Glaois group G has the property that for any $g, h \in G$ with $\mathrm{ord}(g) = \mathrm{ord}(h)$, $< g >$ is conjugate in G with $< h >$, then, if the ideals P_1 and P_2 in the integer ring R of K have the same decomposition in the integer ring S of L, then they have the same decomposition in any intermediate field extension of K.

BAZI ÖZEL CİSİM GENİŞLEMELERİ İÇİN ASAL İDEALLERİN PARÇALANIŞI

Özet : $K \subset L$ bir normal cisim genişlemesi ve G, bu genişlemenin Galois grubu olsun, öyle ki, $\mathrm{ord}(g) = \mathrm{ord}(h)$ koşuluna uyan herhangi bir $g, h \in G$ çifti için $< g >$, G de $< h >$ ile eşlenik olsun. Bu çalışmada, K nın R tam sayılar halkasında P_1 ve P_2 gibi iki idealin, L nin S tam sayılar halkasında aynı parçalanışı haiz olmaları durumunda K nın herhangi bir ara genişlemesinde de aynı parçalanışı haiz oldukları ispat edilmektedir.

Let $K \subset L = K(\alpha)$ algebraic number fields extension, α an element of degree n over K and $R \subset S$, $\alpha \in S$, the corresponding integer rings. Since S and $R(\alpha)$ are finite generated $\mathbf{Z}$-modules with the same rank mn where $m = [K : \mathbf{Q}]$, then, the factor group $S/R(\alpha)$ is finite.

Let P a prime ideal of R and g be the monic irreducible polynominal of α over K. The coefficients of g are algebraic integers, hence they are in R. Let $\mathfrak{g}$ be the corresponding polynomial in $(R/P)[x]$ obtained by reducing the coefficients of g mod P. $\mathfrak{g}$ factors uniquely into monic irreducible factors in $(R/P)[x]$, $\mathfrak{g} = \mathfrak{g}_1^{e_1} \dots \mathfrak{g}_r^{e_r}$ where $\mathfrak{g}_i$ are monic polynomials over R. It is assumed that $\mathfrak{g}_i$ are distinct. Then, the prime decomposition of PS is given by $PS = Q_1^{e_1} \dots Q_r^{e_r}$ where Q_i is the ideal $(P, \mathfrak{g}_i(\alpha))$ in S generated by P and $\mathfrak{g}_i(\alpha)$; in other words $Q_i = PS + (\mathfrak{g}_i(\alpha))$. Also, $f(Q_i \mid P)$ is equal to the degree of g_i (see [1], pg. 79).

Suppose now that $K \subset L$ is normal, $G = \mathrm{Gal}(L : K)$ and P is a prime ideal or R unramified over L ($e_1 = \dots = e_r = 1$). Let Q be a prime ideal of

$PS = Q_1 \dots Q_r$. Then, there is a $\Phi \in G$ (the Frobenius automorphism of Q over P) such that $\Phi(\alpha) \equiv \alpha^{|P|} (\mathrm{mod}\, Q)$, where $|P| = |R/P|$. The conjugacy class of Φ in G is well determined by P. The order of Φ is $\mathrm{ord}(\Phi) = |S/Q : R/P| = f(Q \mid P)$ and $rf(Q \mid P) = n = [L : K]$.

Let now $K \subset L \subset M$ be a field extension with $K \subset M$ normal, $G = \mathrm{Gal}(M : K)$, and $R \subset S \subset T$ be the corresponding integer rings. Let P be a prime ideal of K, unramified over M, $\Phi = \Phi(U \mid P)$ the Frobenius automorphism, where U is a prime ideal of T which appears in the decomposition of PM. Let $H < G$, $H = \mathrm{Gal}(M : L)$. Consider the action of Φ over $(H\sigma \mid \sigma \in G)$ given by $H\sigma \dashrightarrow H\sigma\Phi$. Then, G/H is partitioned into classes of the form $(H\sigma_i, H\sigma_i\Phi, \dots, H\sigma_i\Phi^{m_i-1})$ if $H\sigma_i\Phi^{m_i} - H\sigma$. Then, the decomposition of P over S has the form $PS = Q_1 \dots Q_r$, where $Q_i = (\sigma_i U) \cap S$ and $f(Q_i \mid P) = m_i$. Clearly, we have $\Sigma\, m_i = n = [L : K]$ (see [1], chap. IV). Obviously, the elements of the same conjugacy class of Φ gives the same action on G/H.

Let $g \in G$. By Frobenius density theorem (see [2]) for any conjugacy class of G, there are infinitely many prime ideals P such that $\Phi(Q/P)$ belong to this class.

Let G be a finite group such that for every $g, h \in G$, $< g >$ is conjugate in G to $< h >$. Let S_m be a symmetric group such that G is embedded in S_m. Then, there are L and M number fields such that $L \subset M$ and $\mathrm{Gal}(M : L) = S_m$. Let $K = \mathrm{Inv}\, G \subset M$. Then $\mathrm{Gal}(M : K) = G$. Applying the previous discussion to $K \subset M$ and G, we obtain the following theorem:

Theorem. Let G be a finite group such that for every $g, h \in G$, $< g >$ is conjugate in G to $< h >$. Then, there is a normal number field extension $K \subset M$ with $\mathrm{Gal}(M : K) = G$ such that, if P_1, P_2 are prime ideals in the integer ring R of K which have the same decomposition over the integer ring S of M (that means the decompositions of P_1 and P_2 have the same number of prime ideals in S, $Q_1 \dots Q_r$ resp. $Q'_1, \dots, Q'_r$, having the same inertia degrees $f_i(Q_i \mid P_1) = f_i(Q'_i, P_2)$, $i = 1, \dots, r$), then P_1, P_2 have the same decompositions in any intermediate extension over K (even nonnormal).

REFERENCES

[1] MARKUS, D. : Number Fields, Springer-Verlag, 1977.

[2] NEUKIRCH, J. : Klassenkörpertheorie, Bibliographisches Institut, Mannheim/Wien Zürich, 1969.