Journal of Prime Research in Mathematics Vol. **2***(2006), 198-202*

ON THE ARITHMETIC OF THE RATIONAL FUNCTION FIELD $K(X)$

SARFRAZ AHMAD[1], ANGEL POPESCU[1,2]

Abstract. Let K be a commutative field. In this paper we study the action of the automorphism group of the rational function field $K(X)$ on the set of all valuations of $K(X)$ which are trivial on K. We apply this study in finding a classification of some simple algebraic extension of K.

Key words: Valuation Theory, Algebraic Extensions, Automorphism, Action of groups.
AMS SUBJECT: 16W60, 16W22, 16W20.

Here we begin to study the action of $G = Aut(K(X)/K)$ on the set of discrete rank one valuations of $K(X)$.

Definition 1. *A homogeneous polynomial $P(Z,Y) = a_0Y^n + a_1ZY^{n-1} + ... + a_nZ^n$ of degree n is called an irreducible polynomial if it cannot be decomposed into a product of homogeneous polynomials of degree greater or equal to one.*

Lemma 1. *A polynomial $P(X) = a_0 + a_1X + ... + X^n$ is irreducible in $K[X]$ if and only if $\bar{P}(Z,Y) = a_0Y^n + a_1ZY^{n-1} + ... + a_{n-1}Z^{n-1}Y + Z^n$ is irreducible in the multiplicative monoid $K[Z,Y]^h$ ={all homogeneous polynomials in $K[Z,Y]$}.*

Proof. $\Rightarrow$) Suppose $\bar{P}(Z,Y) = Q_1(Z,Y)Q_2(Z,Y)$ with Q_1, Q_2 of degree ≥ 1. Since $a_0 \neq 0$ and Q_1, Q_2 has the homogeneous degree at least 1, so for $X = Z/Y$, we obtain $\bar{P}(X,1) = P(X) = Q_1(X,1)Q_2(X,1)$, that is a proper decomposition of $P(X)$ in $K[X]$, a contradiction.
$\Leftarrow$) Conversely, if $\bar{P}(Z,Y)$ is irreducible, then a proper decomposition of $P(X) = P_1(X)P_2(X)$ implies a proper decomposition of $\bar{P}(Z,Y) = \bar{P}_1(Z,Y)\bar{P}_2(Z,Y)$, a contradiction. □

[1]School of Mathematical Sciences, GC Unversity, Lahore, 68-B, New Muslim Town, Lahore, Pakistan. E-mail: sarfraz11@gmail.com.
[2]Technical University of Civil Engineering, Bucharest, Romania, E-mail: popescuangel@yahoo.co.uk.

Definition 2. *Let P_1, P_2 be two irreducible polynomials in $K[X]$. Then $P_1 \sim P_2$ if and only if $P_1 = kP_2$ where $k \in K$. The class of all equivalent irreducible polynomials to P is called an irreducible divisor in $K[X]$ and it is denoted by $[P]$.*

Corollary 2. *The mappings $[P(X)] \overset{\theta}{\mapsto} \bar{P}(Z,Y)$ and $[\bar{P}(Z,Y)] \overset{\theta^{-1}}{\mapsto} P(X)$, $X = Z/Y$, give a one-to-one correspondence between the set of irreducible divisors of degree ≥ 2 of $K(X)$ and the set of irreducible divisors of degree ≥ 2 of $K[Z,Y]^h$.*

Remark 1. *In general, let R be a unique factorization domain. A prime divisor of R is an ideal of R generated by an irreducible element Q of R and it gives rise to a unique discrete valuation V_Q of the field of fraction T of R (see 1, 2, 3). In fact V_Q depends only on $[Q]$. Here $Q_1 \in [Q] \Leftrightarrow Q_1 = uQ$ for some unit u in R. Namely, if $\xi \in R$, then $(\xi) = (Q_1^{\alpha_1})(Q_2^{\alpha_2})...(Q_n^{\alpha_n})$, the unique decomposition in R of the ideal generated by ξ into principal ideals generated by some unique power of the irreducible elements $Q_1 = Q, Q_2, ..., Q_n$ of R. We simply put $V_Q(\xi) =$ the exponent of Q in the decomposition of ξ, namely $V_Q(\xi) = \alpha_1$. If $\eta = \frac{\xi_1}{\xi_2}, \xi_1, \xi_2 \in R, \xi_2 \neq 0$, is an element of T, we put $V_Q(\eta) = V_Q(\xi_1) - V_Q(\xi_2)$.*

Lemma 3. *Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$, i.e. $ad - bc \neq 0$ and let $K[Z,Y]^h$ be the multiplication monoid of all homogeneous polynomials in two variables Z and Y with coefficients in K. Let $\varphi : K[Z,Y]^h \to K[X]$ be the following product preserving mapping: $\varphi(\bar{P}(Z,Y)) = \bar{P}(aX + b, cX + d)$ and we denote it by $\bar{\bar{P}}(X)$. Then φ transforms a polynomial of degree n into a polynomial of the same degree n for any $n \geq 2$. The inverse of φ does the same. In particular, $\bar{P}(Z,Y)$ is irreducible in $K[Z,Y]^h$ if and only if $\varphi(\bar{P}(Z,Y))$ is irreducible in $K[X]$.*

Proof. Let us denote by $\psi : K[Z,Y]^h \to K[Z,Y]^h$ defined by $\psi(\bar{P}(Z,Y)) = \bar{P}(aZ + bY, cZ + dY)$. This mapping is an isomorphism and its inverse ψ^{-1} is defined as $\psi^{-1}(\bar{Q}(\acute{Z},\acute{Y})) = \bar{Q}(\acute{a}\acute{Z} + \acute{b}\acute{Y}, \acute{c}\acute{Z} + \acute{d}\acute{Y})$ where $\begin{pmatrix} \acute{a} & \acute{b} \\ \acute{c} & \acute{d} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$. It is easy to see that ψ transforms a homogeneous polynomial of degree n into a homogeneous polynomial of the same degree. Hence ψ and ψ^{-1} transform irreducible polynomials into irreducible polynomials. But φ is the composition $\theta^{-1} \circ \psi$ between the K-algebra isomorphism θ^{-1} from Corollary 2 and the above K-algebra isomorphism ψ. Now all the statements of Lemma 3 become clear. □

Remark 2. *From 2. we know that any (Krull) valuation ν discrete, trivial of K and of rank 1 of $K(X)$, the rational function field in one variable X over the field K, is of the form ν_p(see Remark 1), where P is a monic irreducible polynomial is $K[X]$, the ring of polynomials in one variable over K, or $\nu = \nu_\infty$, where $\nu_\infty(\frac{A}{B}) = degB - degA$ for any $A, B \in K[X]$. Let $Val_{K(X)}$ be the set of all these valuations. From 1. we know that the automorphism group $G = Aut(K(X)/K)$ acts on the set $Val_{K(X)}$ in the following way: $\sigma \in G$, $(\sigma * \nu)(f(X)) = \nu(\sigma(f(X))) = \nu(f(\sigma(X)))$, where $f(X) \in K(X)$. If $\sigma \in Aut(K(X)/K)$, let $\sigma(X) = \frac{aX+b}{cX+d}$, where $ad - bc \neq 0$, we denote $A_\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.*

Lemma 4. *If $\nu \neq \nu_\infty$, then $\sigma * \nu$ is a new (Krull) valuation on $K(X)$. If $\nu = \nu_\infty$, then $\sigma * \nu_\infty$ is well defined if and only if $A_\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, with $ad \neq 0$.*

Proof. a). $(\sigma * \nu)(0) = \nu(0) = \infty$ and $(\sigma * \nu)(f) = \infty \Rightarrow \sigma(f) = 0 \Rightarrow f = 0$.
b). $(\sigma * \nu)(fg) = \nu(\sigma(f)\sigma(g)) = \nu(\sigma(f)) + \nu(\sigma(g)) = (\sigma * \nu)(f) + (\sigma * \nu)(g)$
c). $(\sigma * \nu)(f + g) = \nu(\sigma(f) + \sigma(g) \geq min\{\nu(\sigma(f)), \nu(\sigma(g))\} = min\{(\sigma * \nu)(f), (\sigma * \nu)(g)\}$. If $\nu = \nu_\infty$ and $c \neq 0$, $(\sigma * \nu_\infty)(L(X)) = \nu_\infty(\frac{\bar{\bar{L}}(X)}{(cX+d)^n}) = 0$, where L is any polynomial of $K[X]$ of degree n. If $\nu = \nu_\infty$ and $c = 0$, $\sigma * \nu_\infty = \nu_\infty$. □

Any $\sigma \in G$ is complete defined by a nonsingular 2×2 matrix $A_\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$. The corresponding φ from lemma 3 will be denoted by φ_σ, i.e. $\varphi_\sigma(\bar{P}(Z, Y)) = \bar{P}(aX + b, cX + d) = \bar{\bar{P}}$.

Theorem 5. *Let $[P]$ be a prime divisor of $K(X)$, i.e. the class of an irreducible polynomial P of $K[X]$ or the class of $\frac{1}{X}$(which gives the valution ν_∞). Let $\sigma \in G = Aut(K(X)/K)$ and let $[Q]$, such that $\sigma * \nu_p = \nu_Q$. Then we have the following cases: (a). If $[P] \neq [cX + d]$ and $[p] \neq [\frac{1}{X}]$, then $[Q(X)] = [(\theta^{-1} \circ \psi_\sigma^{-1} \circ \theta)(P)]$. (b) If $[P] = [cX + d]$, then $[Q(X)] = [\frac{1}{X}]$, i.e. $\nu_Q = \nu_\infty$. (c) If $\nu_P = \nu_\infty$, then $\sigma * \nu_\infty$ is well defined if and only if $A_\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, $ad \neq 0$ and in this last case, $\sigma * \nu_\infty = \nu_\infty$, i.e. ν_∞ is a fixed "point" for all such a σ.*

Proof. (a) Let $P(X)$ be a monic irreducible polynomial of $K[X]$ such that $[P] \neq [cX + d]$. Then $\nu_Q(f) = \nu_P(\sigma(f))$ for every $f \in K(X)$. But $\nu_Q(Q) = 1$, so we must compute $\nu_P(\sigma(Q(X))) = 1$, but $\sigma(Q(X)) = Q(\sigma(X)) = \frac{\bar{Q}(aX+b,cX+d)}{(cX+d)^n}$, where $A_\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $degQ = n$. Here we continue to use the same notations as in Lemmas 1 and 3. Namely $\bar{Q}(Z, Y) = \theta(Q(X))$

and $\bar{Q}(aX+b, cX+d) = \varphi_\sigma(\bar{Q}(Z,Y)) = (\varphi_\sigma \circ \theta)(Q(X))$ and again we denote it by $\bar{\bar{Q}}(X)$. Sinc $\nu_P(\sigma(Q(X))) = 1$ we get that $\xi P(X) = \bar{\bar{Q}}(X)$, where $\xi \in K$. Hence $Q(X) = \xi(\theta^{-1} \circ \varphi_\sigma^{-1})(P)$. But $\varphi_\sigma = \theta^{-1} \circ \psi_\sigma$ (see the proof of Lemma 3) and so, $[Q(X)] = [(\theta^{-1} \circ \psi^{-1} \circ \theta)(P)]$.

(b) If [P]=[cX+d], then $\nu_P[\bar{Q}(aX+b, cX+d)] = n+1$, i.e. $\bar{Q}(aX+b, cX+d) = \eta(cX+d)^{n+1}$, with $\eta \in K$. Like in (a), we get that $Q(X) = [(\theta^{-1} \circ \psi_\sigma \circ \theta)(cX+d)]^{n+1} = [\theta^{-1}(Y)]^{n+1} = 1$.

Hence $\sigma * \nu_P$ is no one of the finite valuation ν_Q for an irreducible polynomial Q of $K[X]$. It remains only that $\sigma * \nu_{[cX+d]} = \nu_\infty$.

(c) If $\nu_P = \nu_\infty$ we just did it in Lemma 4. □

Remark 3. *From Theorem 5 we have to consider the action of* $G = Aut(K(X)/K)$ *only on* $val^*_{K(X)} = val_{K(X)} \backslash \{\nu_\infty, \nu_{cX+d}, c \neq 0, c, d \in K\}$. *We shall simply identify the valuation* $\nu_P \in val^*_{K(X)}$ *with the monic irreducible polynomial* P *of degree* ≥ 2. *We simply define* $\sigma * P(X) = \bar{\bar{P}}(X)$, *with the notations from Lemma 3.*

Theorem 6. *Let* $val^*_{K(X),n}$ *be the valuations which comes from all the monic irreducible polynomials of degree* n, $n \geq 2$. *Then for any* $\sigma \in G$, $\sigma * val^*_{K(X),n} = val^*_{K(X),n}$.

Proof. This equality is a simple consequence of Theorem 5 (a) namely, the equaltiy $[Q(X)] = [(\theta^{-1} \circ \psi_\sigma^{-1} \circ \theta)(P(X))]$ or $P(X) = (\theta^{-1} \circ \psi_\sigma \circ \theta)(Q(X))$. □

Remark 4. *The result of Theorem 6 deos not mean that the action "*" is transitive. For instance, it is not difficult of prove that there does not exist a* $\sigma \in G$ *such that* $[\sigma * (x^3+2)] = [x^3+3]$, *when* $K = Q$. *In the same way, if* $P = X^2 + B$ *and* $Q = X^2 + C$, $B \neq C$, *then does not exist a* $\sigma \in G$ *such that* $[\sigma * P] = [Q]$. *A very interesting question is to study the orbits of* G *on* $val^*_{K(X),2}, val^*_{K(X),3}, \ldots$.

Let $\alpha \in \bar{K}$, a fixed algebraic closure of K, be a root of a monic irreducible polynomial $P(X) \in K[X]$, $\alpha \notin K$. Let $\sigma \in G$, $A_\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, be an element of G. Let $\beta \in \bar{K}$, be defined by the equality $\alpha = \frac{a\beta+b}{c\beta+d}$. Let $\bar{P}(Z,Y) = \theta(P(X))$. Then $\bar{P}(\alpha, 1) = 0$. But $\bar{\bar{P}}(X) = \bar{P}(aX+b, cX+d) = (cX+d)^{degp} P(\frac{aX+b}{cX+d})$. Since $\beta \notin K$, one has that $\bar{\bar{P}}(\beta) = 0$ ($P(\alpha) = 0!$), i.e. β is a root of $\bar{\bar{P}}(X)$. Let denote by Σ_α the mapping $P(X) \mapsto \bar{\bar{P}}(X)$ defined by $\sigma \in G$. We obtained in fact the following result:

Theorem 7. *If* $\sigma \in G$, $A_\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, *then* $\alpha \notin K$ *is a root of the monic irreducible polynomial* $P(X) \in K[X]$ *if and only if* $\beta \in \bar{K}$ *defined by the formula* $\alpha = \frac{a\beta+b}{c\beta+d}$ *is a root of* $\bar{\bar{P}}(X) = \Sigma_\alpha(P(X))$, *In particular* $K(\alpha) = K(\beta)$.

This is a criteria to describe the orbit of the action of "*" on a given subset $val^*_{K(X),n}$, where $n \geq 2$. Morover, for $n = 2$ we even obtain a criteria for saying when two algebraic extension of degree 2 of K are identical. Indeed, if $L \cong K[X]/(P(X))$ and $M \cong K[X]/(Q(X))$ are extensions of degree 2 over K, then $L = M$ if and only if the irreducible polynomials $P(X)$ and $Q(X)$ belongs to the same orbit of action "*".

References

1. P.J.McCarthy, *Algebraic Extensions of Fields*, Blaisdell Publishing Company, 1966.
2. N. Jacobson, *Lectures in Abstract Algebra*, Vol III, Springer-Verlag, N.Y., 1964.
3. O. Zariski, P. Samuel, *Commutative Algebra*, Vol I, II, D. van Nostrand Company, Inc., Princetin, 1958.
4. J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, 1999.