Takehiko Miyata**J
Nagoya Math. J.
Vol. 41 (1971), 69–73

INVARIANTS OF CERTAIN GROUPS I[1)]

TAKEHIKO MIYATA[2)]

Let G be a group and let k be a field. *A* k-representation ρ of G is a homomorphism of G into the group of non-singular linear transformations of some finite-dimensional vector space V over k. Let K be the field of fractions of the symmetric algebra $S(V)$ of V, then G acts naturally on K as k-automorphisms. There is a natural inclusion map $V \to K$, so we view V as a k-subvector space of K. Let $v_1, v_2, \cdots, v_n$ be a basis for V, then K is generated by $v_1, v_2, \cdots, v_n$ over k as a field and these are algebraically independent over k, that is, K is a rational field over k with the transcendence degree n. All elements of K fixed by G form a subfield of K. We denote this subfield by K^G.

We say that ρ *has the property* $[R]$ *if* K^G *is a rational field over* k.

Kuniyoshi proved that if G is a finite p-group and if k is a field of characteristic p, the regular representation has the property $[R]$ ([3]). Gaschütz generalized this result to an arbitrary representations ([2]). We shall give other generalizations of their results.

Let G be a group and let ρ be a k-representation of G. Let V be the underlying space of this representation. ρ is called triangularizable if there exisrs a G-invariant flag[3)] in V.

Followings are examples of triangularizable representations:

(1) G is a finite commutative group of exponent m and k is a field whose characteristic does not divide m and which contains a primitive m-th root of unity. Then every k-representation of G is triangulariazble.

Received September 29, 1969.

1) This is a part of the author's thesis written under the guidance of Professor Heisuke Hironaka at Columbia University.

2) The author wants to thank Professors H. Hironaka and H. Matsumura who encouraged him constantly during this research. He also wants to thank Professor R. Friedberg and Dr. L. Olson who helped the author in writing English.

3) *A* flag F in V is a sequence of subspaces of V F: $V = V_n \supset V_{n-2} \supset \cdots V_1 \supset V_0 = (0)$ such that $\dim V_i = i$ $(n = \dim V)$. F is G-invariant if $\rho(g)(V_i) \subset V_i$ for all $g \in G$ and all i.

https://doi.org/10.1017/S0027763000014069 Published online by Cambridge University Press

(2) G is a finite p-group where p is a prime number and k is an arbitrary field of characteristic p. Then every k-representation of G is triangulariazble.

Since there is no adequate reference, we give a sketch of a proof. Let V be a representation space of G. It suffices to show that there exists a non-zero G-invariant element in V. Since G is a p-group, there exists an element g of order p in the center of G. It is immediate that $(\rho(g))-1)^p=0$. Therefore, there exists an integer i $(0 \leq i < p)$ such that $V' = (\rho(g)-1)^i V \neq 0$ and $(\rho(g)) - 1)V' = (\rho(g) - 1)^{i+1}V = 0$. An element in V' is G-invariant. Let V_0 be the subspace consisting of all G-invariant elements in V_0. Since g is in the center of G, $G/\langle g\rangle$ acts on V_0 naturally. By mathematical induction on the order of G, V_0 has a non-zero $G/\langle g\rangle$-invariant (hence, G-invariant) element.

(3) (Lie-Kolchin) G is a connected solvable algebraic group over an algebraically closed field. Then any rational representation of G is triangularizable. ([1], Theorem 10.4).

(4) G is a connected solvabletopological group. Then every continuous representation on a finite dimensional vector space over the complex number field is triangularizable. ([6], Theorem 5.1*, Lemma 5.11).

THEOREM 1. *Let G be a group and let k be a field. Then every triangularizable k-representation of G has the property* (R).

By the triangularizability, the problem reduces by induction to proving

LEMMA. *Let G be a group acting on a field K. If G acts also on a polynomial ring of one variable $K[t]$ in the following way:*

$$g(t) = \lambda(g)t + \mu(g), \quad g \in G$$

where $\lambda(g)$ $(\neq 0)$ and $\mu(g)$ belong to K, then there exists an element x in $K[t]$ such that $K(K(t)^G) = K(x)$.

Proof. First of all we show that the field of fractions K' of $K[t]^G$ is $K(t)^G$. Let $F/L \in K(t)^G$, F, $L \in K[t]$. We prove that F/L belongs to K' by the induction on $\deg(F) + \deg(L)$ where deg. means the degree in t. If $\deg(F)$ or $\deg(L)$ is zero, there is nothing to prove. Suppose that $\deg(F)$ and $\deg(L)$ are positive and that F and L are relatively prime. Since $K[t]$ is a unique factorization domain, we have

$$g(F) = \chi(g)F, \quad g(L) = \chi(g)L,$$

where $\chi(g)$ is a character of G with values in K^*. We may assume $\deg(F) \geqq \deg(L)$. Dividing F by L we have

$$F = S \cdot L + R \quad \deg(R) < \deg(L).$$

applying g in G, we get

$$\chi(g)F = \chi(g)\,(g(S))L + g(R).$$

Since $\deg(F) = \deg(g(F))$ and $\deg(L) = \deg(g(L))$, we see that $g(S) = S$ and $g(R) = \chi(g)R$ by the uniqueness of division. By the induction assumption, $R/L \in K'$, hence F/L belongs to K'.

Now this observation shows us that if $K[t]^G \subset K$, then $K(t)^G \subset K$. If $K[t]^G \subset K$, there is nothing to prove. If $K[t]^G \not\subset K$, then choose $x \in K[t]^G - K$ such that $\deg(x)$ is minimal. Then by an argument similar to that in the above observation, we can show that an element in $K[t]^G$ is a polynomial in x with coefficients in K^G, that is, $K[t]^G = K^G[x]$. q.e.d.

Remark 1. This lemma is a generalization of Hilbert's Theorem 90. In fact, let G be a *finite* group of field automorphisms of K and let $\mu(g)$ (resp. $\lambda(g)$) be an additive (resp. multiplicative) cocycle of G with values in K (resp. K^*). Then by defining $g(t) = t + \mu(g)$ (resp. $g(t) = \lambda(g)t$) G acts on the polynomial ring $K[t]$. It is easy to see that $K(K(t)^G) = K(t)$ by the fundamental theorem of Galois theory. By Lemma there is an element x in $K[t]^G$ such that $K(t) = K(x)$. x must be linear in t, say $at + b$, a, $b \in K$. Now $at + b = g(a)g(t) + g(b)$, for all g in G, so $at + b = g(a)\,(t + \mu(g)) + g(b)$ (resp. $at + b = g(a)\lambda(g)t + g(b)$). Hence $\mu(g) = b/a - g(b/a)$ (resp. $\lambda(g) = a\,g(a)^{-1}$). This means $H^1(G, K) = (0)$ (resp. $H^1(G, K^*) = (1)$).

Remark 2. One might be tempted to formulate the lemma in the following way;

Let K_1 be a subfield of a rational field $K(t)$ of one variable (K_1 not necessarily containing K). Then there is an element x in K_1 such that $K(K_1) = K(x)$.

Unfortunately this is not true in general.

Let $K = K(s)$ be a rational field of one variable over a field k. Let $K_1 = k(t^2, t^3 + s)$, where t is an indeterminate. Then this is a counter example.

Proof. We note that $k(s)(t^2, t^3+s) = k(s, t)$. Suppose that we find an element x in K_1 such that $k(s)(K_1) = k(s)(x)$. Then.

$$x = \frac{\alpha t+\beta}{\gamma t+\delta} \quad \alpha\delta - \beta\gamma \neq 0, \quad \alpha, \beta, \gamma, \delta \in k[s].$$

We may assume that $\alpha \neq 0$. Put $u = t^2$ and $v = t^3 + s$. We can write $F/L = (\alpha t+\beta)/(\gamma t+\delta)$ where F and L belong to $K[u, v]$. Let F_0, L_0 be the constant terms in F, L as polynomials of t then since

$$(\gamma t+\delta)F(u, v) \equiv (\alpha t+\beta)L(u, v) \bmod (t^2),$$

we get that $\delta F_0 = \beta L_0$ and $\gamma F_0 = \alpha L_0$. Therefore $(\alpha\delta - \beta\gamma)F_0 = \alpha(\delta F_0) - \beta(\gamma F_0) = 0$. This is a contradiction, if $F_0 \neq 0$.

If $F_0 = 0$, then $F(u, v) = F'(u, v)u^m$ where F' has non-zero constant term. In fact, write.

$$F(u, v) = F'(u, v)u + F''(v), \quad F' \in K[u, v], \quad F'' \in k[v].$$

Since F has no non-zero cnostant term as a polynomial in t, $0 = F(0, s) = F''(s)$, hence $F'' \equiv 0$. Now by this observation we may assume that $F_0 \neq 0$.
q.e.d.

Remark 3. Let V be an underlying space of a k-representation of a *finite* group G. Suppose that V has a *faithful* sub-G-module W which has the property (R), then V has the property (R).

Proof. Let $w_1, w_2, \cdots, w_m$ be a basis for W. We may identify the symmetric algebra $S(W)$ with the polynomial ring $k[w_1, w_2, \cdots, w_m]$. Let K be the field of fractions of $S(W)$. Let $v_1, v_2, \cdots, v_n$ be vectors in V such that they together with $w_1, w_2, \cdots, w_m$ form a basis for V. Let K' be the field of fractions of $S(V) = k[w_1, \cdots, w_m, v_1, \cdots, v_n]$. Then we show that there exist n elements $x_1, x_2, \cdots, x_n$ in K'^G such that $K(K'^G) = K(x_1, x_2, \cdots, x_n)$ $(=K')$. In fact, the action of an element g in G on K' is

$$g\begin{pmatrix} v_1 \\ \vdots \\ v_n \\ 1 \end{pmatrix} = \begin{pmatrix} & & a_1(g) \\ & A_0(g) & \vdots \\ & & a_n(g) \\ 0 \cdots\cdots 0 & & 0 \end{pmatrix} \begin{pmatrix} v_1 \\ \\ v_n \\ 1 \end{pmatrix}$$

where $A_0(g) \in GL(n, k) \subset GL(n, K)$ and $a_i(g) \in K$. Let H be the subgroup of

https://doi.org/10.1017/S0027763000014069 Published online by Cambridge University Press

$GL(n+1, K)$ consisting of elements of the type $\begin{bmatrix} A_0 & * \\ 0 & 1 \end{bmatrix}$. We let G act on $GL(n+1, K)$ coefficientwise, then H is G-stable. If we write $(v) = {}^t(v_1, \cdots, v_n, 1)$ and $A(g) = \begin{bmatrix} A_0(g) & * \\ 0 & 1 \end{bmatrix}$, then $(hg)(v) = A(hg)(v) = h(g(v)) = {}^hA(g)A(h)(v)$. Therefore, $g \to A(g)^{-1}$ is a cocycle of G with values in H. There is an exact sequence

$$(1) \to \underbrace{K \times \cdots \times K}_{n\text{-tuples}} \to H \to GL(n, K) \to (1)$$

Since $H^1(G, K)$ and $H'(G, GL(h, K))$ are trivial (by assumption, G is finite and the action of G on K is faithful), $H^1(G, H) = (1)$ ([5], p. 133). This means that there exists $B \in H$ such that $A(g) = {}^gB \cdot B^{-1}$. If we set $(x) = {}^t(x_1, \cdots, x_n, 1) = B^{-1}(v)$, then $g(x) = {}^gB^{-1} \cdot g(v) = {}^gB^{-1}A(g)(v) = B^{-1}(v) = (x)$. x_i's satisfy the property. q.e.d.

THEOREM 2. *A two dimensional representation has the property* (R). *A three dimensional representation has the property* (R) *if* k *is algebraically closed.*

This theorem is essentially due to Noether ([4], § 2)

Proof. Let V be a representation space of a group G and let $x_1, \cdots, x_n$ be a basis of V.

$$K = k(V) = k(x_2 x_1^{-1}, \cdots, x_n x_1^{-1})(x_1).$$

Since $K_1 = k(x_2 x_1^{-1}, \cdots, x_n x_1^{-1})$ is G-stable and $g(x_1) = (g(x_1)x_1^{-1})x_1$, there exists an element $z \in K^G$ such that $K^G = K_1^G(z)$ by Lemma. If $\dim V = 2$, the theorem follows from Lüroth's theorem and if $\dim V = 3$, the theorem follows from Zariski-Castelnuovo's theorem. q.e.d.

REFERENCES

[1] Borel, A.; Groupes algébriques linéaires. Annals of Math. (2) **64,** 20–82 (1956).
[2] Gaschutz, W., Fixkörper von p-automorphismengruppen rein transzendenter Korpererweiterungen von p-Charakteristik. Math. Z., Vol. **71** (1969).
[3] Kuniyoshi, H.; Certain subfields of rational function fields. Proc. International Sym. on Algebraic Number Theory, 241–243 (1955).
[4] Noether, E.; Gleichungen mit vorgebshriebene Gruppe. Math. Ann. **78,** 221–229 (1916).
[5] Serre, J. -P.; Corps locaux. Paris.
[6] ————; Lie algebras and Lie groupes. Benjamin,

Research Institute for Mathematical Sciences, Kyoto University.