# On generic cyclic polynomials of odd prime degree 

By Shin Nakano<br>Department of Mathematics, Gakushuin University, 1-5-1, Mejiro, Toshima-ku, Tokyo 171-8588<br>(Communicated by Shokichi Iyanaga, m. J. a., Dec. 12, 2000)


#### Abstract

Using Cohen's construction of defining polynomials for a cyclic group of odd prime order, we define a polynomial with some parameters which generates cyclic extensions of a given odd prime degree, and prove it to be generic in the sense as defined below.


Key words: Generic polynomial; cyclic extension.

1. Introduction. Let $k$ be a field and $\mathfrak{G}$ a finite group. A polynomial over $k$ with some parameters is called a generic polynomial for $\mathfrak{G}$ if it generates all Galois extensions with Galois group $\mathfrak{G}$ over an arbitrary extension of $k$ by specializations of the parameters. Let $C_{l}$ be the cyclic group of an odd prime order $l$. The aim of this paper is to investigate generic polynomials for $C_{l}$ over $k$ of characteristic other than $l$. The result of Saltman [4] implies the existence of a polynomial of this kind. The simplest example is given by Kummer theory. In fact, if $k$ contains an $l$-th root of unity then $X^{l}-T$ is a generic polynomial with one parameter $T$ for $C_{l}$. Moreover, in case $k=\mathbf{Q}$, an explicit construction for a generic polynomial for $C_{l}$ was essentially given by Smith [6]. On the other hand, Cohen [1] gave a method of generating cyclic polynomials of degree $l$, by using a simple tool of Kummer theory, which seems to us more natural and more easily comprehensible than Smith's. In the present paper, largely following Cohen's method, we will construct a polynomial over $k$ of degree $l$ with some parameters, and prove this polynomial to be generic over $k$ for $C_{l}$. Our result can be regarded a natural generalization of Smith [6] as well as of the above fact on Kummer theory for the group $C_{l}$.

## 2. Definition of cyclic polynomials.

Throughout this paper, we will fix an odd prime $l$. In this section, we summarize the results on the defining polynomials for cyclic extensions of degree $l$ described in Cohen [1, Ch. 5].

Let $k$ be a field of characteristic other than $l$. Let $\zeta$ be a fixed primitive $l$-th root of unity and put $F=k(\zeta)$. Put $V=F^{\times} / F^{\times l}$ which will be regarded as a vector space over $\mathbf{F}_{l}=\mathbf{Z} / l \mathbf{Z}$. Let $F^{\times} \rightarrow V, \alpha \mapsto$

[^0]$\bar{\alpha}$ be the canonical surjection. Any cyclic extension of degree $l$ over $F$ is given in the form $F(\sqrt[l]{\alpha})$ for some $\alpha \in F^{\times}$. By Kummer theory, this induces a bijection between such cyclic extensions and onedimensional subspaces of $V$. Now the Galois group $G$ of the extension $F / k$ is isomorphic to a subgroup of $\mathbf{F}_{l}^{\times}$under the isomorphism $\chi$ from $G$ into $\mathbf{F}_{l}^{\times}$by $\zeta^{\sigma}=$ $\zeta^{\chi(\sigma)}(\sigma \in G)$. Let $d$ be the order of $G$, that is, $d=$ [ $F: k]$. The Galois group $G$ acts on $V$, and therefore $V$ is an $\mathbf{F}_{l}[G]$-module. Define an idempotent $\varepsilon$ of the group algebra $\mathbf{F}_{l}[G]$ by
$$
\varepsilon=\frac{1}{d} \sum_{\sigma \in G} \chi\left(\sigma^{-1}\right) \sigma
$$

Then the image $V^{\varepsilon}$ of the $\mathbf{F}_{l}$-linear transformation $\varepsilon$ on $V$ is the eigenspace of the generator $\sigma_{0}$ of $G$ with the eigenvalue $\chi\left(\sigma_{0}\right)$. Thus we have

$$
\bar{\alpha} \in V^{\varepsilon} \quad \Longleftrightarrow \quad \bar{\alpha}^{\sigma}=\bar{\alpha}^{\chi(\sigma)} \quad(\sigma \in G)
$$

for $\alpha \in F^{\times}$.
The following two propositions and the definition of cyclic polynomials are all included in Theorem 5.3.5 of [1]; nevertheless, we shall restate a partial result of this theorem as Proposition 2, and give a proof, because we will use the same discussion later on.

Proposition 1. If $K$ is a cyclic extension over $k$ of degree $l$, and $\alpha$ is an element of $F^{\times}$such that $K(\zeta)=F(\sqrt[l]{\alpha})$, then we have $\bar{\alpha} \in V^{\varepsilon}$. Conversely, for $\alpha \in F^{\times}$satisfying $\bar{\alpha} \in V^{\varepsilon} \backslash\{1\}, F(\sqrt[l]{\alpha})$ is an abelian extension over $k$ of degree dl which contains a unique cyclic extension $K$ over $k$ of degree $l$.

This implies that there is a bijection between cyclic extensions over $k$ of degree $l$ and onedimensional subspaces of $V^{\varepsilon}$.

Proposition 2. Let $K$ be a cyclic extension over $k$ of degree $l$ and take $\alpha \in F^{\times}$such that $K(\zeta)=F(\sqrt[l]{\alpha})$. Set $A=\sqrt[l]{\alpha}$ and $L=K(\zeta)$. Then $K=k\left(\operatorname{Tr}_{L / K}(A)\right)$ and all the conjugates of $\operatorname{Tr}_{L / K}(A)$ over $k$ are given by $\operatorname{Tr}_{L / K}\left(A \zeta^{i}\right) \quad(0 \leq i \leq$ $l-1)$.

Proof. We identify the Galois group of $L / K$ with $G$. For each $\sigma \in G$, take an integer $x_{\sigma} \in$ $\{1,2, \ldots, l-1\}$ with $\chi(\sigma)=x_{\sigma} \bmod l$. Since $\bar{\alpha} \in V^{\varepsilon}$ by Proposition 1, we have $\left(A^{\sigma-x_{\sigma}}\right)^{l}=\alpha^{\sigma-x_{\sigma}} \in F^{\times l}$. Thus there is $\gamma_{\sigma} \in F^{\times}$such that $A^{\sigma}=\gamma_{\sigma} A^{x_{\sigma}}$ for $\sigma \in G$. Then we have

$$
\operatorname{Tr}_{L / K}(A)=\sum_{\sigma \in G} \gamma_{\sigma} A^{x_{\sigma}} \notin k
$$

because $\left\{x_{\sigma}\right\}_{\sigma \in G} \subset\{1,2, \ldots, l-1\}$ and $1, A, A^{2}, \ldots$, $A^{l-1}$ are linearly independent over $F$. Hence we have $K=k\left(\operatorname{Tr}_{L / K}(A)\right)$. It is obvious that $\operatorname{Tr}_{L / K}\left(A \zeta^{i}\right)$ are the conjugates of $\operatorname{Tr}_{L / K}(A)$ over $k$. Moreover, if $0 \leq i \neq j \leq l-1$ then

$$
\begin{aligned}
\operatorname{Tr}_{L / K} & \left(A \zeta^{i}\right)-\operatorname{Tr}_{L / K}\left(A \zeta^{j}\right) \\
& =\sum_{\sigma \in G} \gamma_{\sigma}\left(\zeta^{i x_{\sigma}}-\zeta^{j x_{\sigma}}\right) A^{x_{\sigma}} \neq 0
\end{aligned}
$$

which completes the proof.
Under the notations in Proposition 2, we denote by $f(X ; \alpha)$ the minimal polynomial of $\operatorname{Tr}_{L / K}(A)$ over $k$, that is,

$$
f(X ; \alpha)=\prod_{i=0}^{l-1}\left(X-\operatorname{Tr}_{L / K}\left(A \zeta^{i}\right)\right)
$$

Also when $\alpha \in F^{\times l}$, replacing $L, K$ by $F, k$ respectively, we define $f(X ; \alpha)$ in the same form; the product of linear factors $X-\operatorname{Tr}_{F / k}\left(A \zeta^{i}\right)(0 \leq i \leq l-1)$. Obviously, $f(X ; \alpha)$ depends only on $\alpha$ and not on the choice of $A$.

$$
\begin{aligned}
& \text { Let } \\
& \mathcal{E}=\left\{e \in \mathbf{Z}[G] \mid s \varepsilon=e \bmod l \text { for some } s \in \mathbf{F}_{l}^{\times}\right\} .
\end{aligned}
$$

For any $e \in \mathcal{E}$ and $\beta \in F^{\times}$, we can define a polynomial $f\left(X ; \beta^{e}\right)$. In case $\beta^{e} \notin F^{\times l}$, there is a unique subfield $K$ of $L=F(A)$ which is cyclic over $k$ of degree $l$, where $A^{l}=\beta^{e}$. Note that the cyclic extension generated by $f\left(X ; \beta^{e}\right)$ is independent of the choice of $e \in \mathcal{E}$.

Now we take a basis $\left(w_{\sigma}\right)_{\sigma \in G}$ of $F / k$. Let $\boldsymbol{T}=\left(T_{\sigma}\right)_{\sigma \in G}$ be independent transcendentals over $k$ indexed by $G$. The Galois group of $F(\boldsymbol{T}) / k(\boldsymbol{T})$ is canonically isomorphic to $G$. Then we can apply the
above discussion to define a polynomial over $k(\boldsymbol{T})$ by

$$
g(X ; \boldsymbol{T})=f\left(X ; \tilde{\beta}(\boldsymbol{T})^{e}\right)
$$

where

$$
\tilde{\beta}(\boldsymbol{T})=\sum_{\sigma \in G} w_{\sigma} T_{\sigma} \in F(\boldsymbol{T})
$$

Putting $\beta=\tilde{\beta}(\boldsymbol{t})$ for $\boldsymbol{t}=\left(t_{\sigma}\right)_{\sigma \in G} \in k^{d}$, we get again $f\left(X ; \beta^{e}\right)=g(X ; \boldsymbol{t}) \in k[X]$. Therefore all the cyclic extensions over $k$ of degree $l$ are parameterized by $g(X ; \boldsymbol{T})$. Thus we have the following result.

Proposition 3. Any cyclic extension $K$ over $k$ of degree $l$ may be obtained as the splitting field of $g(X ; \boldsymbol{t})$ over $k$ for some $\boldsymbol{t} \in k^{d}$.

Remark. Smith [6] and Dentzer [2] discuss the cyclic polynomials of general odd degrees over $\mathbf{Q}$. If we restrict the degrees to be prime, say $l$, then the polynomials they have constructed are obtained from our $g(X ; \boldsymbol{T})$. Consider $k$ to be $\mathbf{Q}$. In this case we have $d=l-1$ and $G \simeq \mathbf{F}_{l}^{\times}$. Choose $e=\sum_{\sigma \in G} e_{\sigma} \sigma \in$ $\mathcal{E}$ with $e_{\sigma} \in \mathbf{Z}$ satisfying

$$
\chi\left(\sigma^{-1}\right)=e_{\sigma} \bmod l \quad \text { and } \quad 1 \leq e_{\sigma} \leq l-1
$$

and a basis of $F / k$ such as

$$
\left\{w_{\sigma}\right\}_{\sigma \in G}=\left\{\zeta, \zeta^{2}, \ldots, \zeta^{l-1}\right\}
$$

Then it can be verified that $g(X ; \boldsymbol{T})$ coincides with the polynomial that Smith and Dentzer have treated. Though the degrees are restricted to primes, our construction seems more natural to us.
3. A generic polynomial. We will fix $e \in \mathcal{E}$ and a basis $\left(w_{\sigma}\right)_{\sigma \in G}$ of $F / k$. We have constructed with them the polynomial $g(X ; \boldsymbol{T}) \in k(\boldsymbol{T})[X]$ that parameterizes all the cyclic extension over $k$ of degree $l$. Our goal of this section is to prove that $g(X ; \boldsymbol{T})$ is generic over $k$, in other words, $g(X ; \boldsymbol{T})$ has the following properties:
(A) The Galois group of $g(X ; \boldsymbol{T})$ over $k(\boldsymbol{T})$ is cyclic of order $l$.
(B) For any field $k_{1}$ containing $k$ as a subfield and any cyclic extension $K_{1}$ of degree $l$ over $k_{1}$, there exists $t \in k_{1}^{d}$ such that $K_{1}$ is the splitting field of $g(X ; \boldsymbol{t})$ over $k_{1}$.
(For the definition of the term "generic" in a more general situation, see [3]-[6].)

Theorem. The polynomial $g(X ; \boldsymbol{T})$ is generic over $k$, i.e., $g(X ; \boldsymbol{T})$ has the properties (A) and (B).

Before proving the theorem, we analyze the roots of the polynomial $g(X ; \boldsymbol{T})$ and its specialization. We review the discussion in the proof of Propo-
sition 2 and the definition of $f\left(X ; \beta^{e}\right)$. Let $\tilde{A}$ be an element of the algebraic closure of $k(\boldsymbol{T})$ satisfying $\tilde{A}^{l}=\tilde{\beta}(\boldsymbol{T})^{e}$, and put $\tilde{L}=F(\boldsymbol{T})(\tilde{A})$. Let $\tilde{K}$ be the intermediate field of $\tilde{L} / k(\boldsymbol{T})$ such that $[\tilde{L}: \tilde{K}]=d$. The Galois group of $\tilde{L} / \tilde{K}$ is identified with $G$. Let $\sigma \in G$. Take integers $1 \leq x_{\sigma} \leq l-1$ such that $\chi(\sigma)=x_{\sigma} \bmod l$. Then there is the rational function $\tilde{\gamma}_{\sigma}(\boldsymbol{T}) \in F(\boldsymbol{T})$ determined by $\tilde{A}^{\sigma}=\tilde{\gamma}_{\sigma}(\boldsymbol{T}) \tilde{A}^{x_{\sigma}}$. It is not difficult to show that $\tilde{\gamma}_{\sigma}(\boldsymbol{T})$ is independent of the choice of $\tilde{A}$. Using these notations, we obtain the roots of $g(X ; \boldsymbol{T})$ in the form

$$
\operatorname{Tr}_{\tilde{L} / \tilde{K}}\left(\tilde{A} \zeta^{j}\right)=\sum_{\sigma \in G} \tilde{\gamma}_{\sigma}(\boldsymbol{T}) \tilde{A}^{x_{\sigma}} \zeta^{j \sigma}, \quad 0 \leq j \leq l-1
$$

We now denote by $B_{\sigma}(\boldsymbol{T})$ the linear form given by $\tilde{\beta}(\boldsymbol{T})^{\sigma}$ for $\sigma \in G$ :

$$
B_{\sigma}(\boldsymbol{T})=\sum_{\tau \in G} w_{\tau}^{\sigma} T_{\tau}
$$

Write

$$
e=\sum_{\sigma \in G} e_{\sigma} \sigma \quad \text { with } \quad e_{\sigma} \in \mathbf{Z}
$$

Then we have

$$
\tilde{A}^{l}=\tilde{\beta}(\boldsymbol{T})^{e}=\prod_{\sigma \in G} B_{\sigma}(\boldsymbol{T})^{e_{\sigma}}
$$

We need the following two lemmas.
Lemma 1. Any coefficient of $g(X ; \boldsymbol{T})$ is given in the form of a finite sum $\sum q_{i} \tilde{\beta}(\boldsymbol{T})^{u_{i}}$, where $q_{i}$ are elements of the prime field contained in $k$ and $u_{i} \in \mathbf{Z}[G]$.

Proof. See Cohen [1, Proposition 5.3.9].
Lemma 2. Let $k_{1}$ be a field containing $k$ as a subfield and $\boldsymbol{t} \in k_{1}^{d}$. Assume that $B_{\sigma}(\boldsymbol{t}) \neq 0$ for any $\sigma \in G$.
(1) The coefficients of $g(X ; \boldsymbol{T})$ can be defined at $\boldsymbol{t}$, and therefore we obtain a polynomial $g(X ; \boldsymbol{t})$ over $k_{1}$.
(2) For each $\sigma \in G$, the rational function $\tilde{\gamma}_{\sigma}(\boldsymbol{T})$ can be defined at $\boldsymbol{t}$, and $\tilde{\gamma}_{\sigma}(\boldsymbol{t}) \neq 0$.
(3) Let $A_{1}$ be an element of the algebraic closure of $k_{1}$ satisfying

$$
A_{1}^{l}=\prod_{\sigma \in G} B_{\sigma}(\boldsymbol{t})^{e_{\sigma}}
$$

Then all the roots of $g(X ; \boldsymbol{t})$ are given by

$$
\sum_{\sigma \in G} \tilde{\gamma}_{\sigma}(\boldsymbol{t}) A_{1}^{x_{\sigma}} \zeta^{j \sigma}, \quad 0 \leq j \leq l-1
$$

Proof. (1) From Lemma 1, it suffices to show that $\tilde{\beta}(\boldsymbol{t})^{u}$ can be defined for any $u \in \mathbf{Z}[G]$. But,
writing $u=\sum_{\sigma} u_{\sigma} \sigma\left(u_{\sigma} \in \mathbf{Z}\right)$, we confirm that $\tilde{\beta}(\boldsymbol{T})^{u}=\prod_{\sigma} B_{\sigma}(\boldsymbol{T})^{u_{\sigma}}$ can be defined at $\boldsymbol{t}$ satisfying our assumption, also when $u_{\sigma}$ is negative for some $\sigma$.
(2) Since $\tilde{\gamma}_{\sigma}(\boldsymbol{T})^{l}=\tilde{A}^{l\left(\sigma-x_{\sigma}\right)}=\tilde{\beta}(\boldsymbol{T})^{e\left(\sigma-x_{\sigma}\right)}$ and $e\left(\sigma-x_{\sigma}\right) \equiv 0(\bmod l)$, there exist $j_{\sigma} \in \mathbf{F}_{l}^{\times}$and $v_{\sigma} \in \mathbf{Z}[G]$ such that $\tilde{\gamma}_{\sigma}(\boldsymbol{T})=\zeta^{j_{\sigma}} \tilde{\beta}(\boldsymbol{T})^{v_{\sigma}}$. Therefore, in the same manner as in (1), we see that $\tilde{\gamma}_{\sigma}(\boldsymbol{t})$ can be defined, and that $\tilde{\gamma}_{\sigma}(\boldsymbol{t}) \neq 0$.
(3) By specialization, our assertion follows from the above argument on the roots of $g(X ; \boldsymbol{T})$.

We are now ready to prove the main theorem.
Proof of Theorem. Let $W$ be the matrix $\left(w_{\tau}^{\sigma}\right)_{\sigma, \tau \in G}$ (index the rows by $\sigma$, the columns by $\tau$ ). We note that $W$ is regular, since $F / k$ is separable. Thus the $d$ linear forms $B_{\sigma}(\boldsymbol{T})(\sigma \in G)$ are distinct from each other. Therefore $\tilde{\beta}(\boldsymbol{T})^{e}=\prod B_{\sigma}(\boldsymbol{T})^{e_{\sigma}} \notin$ $F(\boldsymbol{T})^{\times l}$ which implies the property (A). Next, let $k_{1}$ be any field extension of $k$ and $K_{1} / k_{1}$ any cyclic extension of degree $l$. To show the property (B), we have to find out $\boldsymbol{t}=\left(t_{\sigma}\right)_{\sigma \in G}$ in $k_{1}^{d}$ such that $K_{1}$ is the splitting field of $g(X ; \boldsymbol{t})$ over $k_{1}$. Let $F_{1}=k_{1}(\zeta)$ and $L_{1}=K_{1}(\zeta)$. The Galois group $H$ of the extension $F_{1} / k_{1}$ is regarded as a subgroup of $G$ naturally. Put

$$
e(H)=\sum_{\sigma \in H} e_{\sigma} \sigma
$$

Since $L_{1}$ is abelian over $k_{1}$, there is $\beta_{1} \in F_{1}^{\times}$such that $L_{1}=F_{1}\left(A_{1}\right)$ where $A_{1}^{l}=\beta_{1}^{e(H)}$ by Proposition 1. For $\sigma \in G$, set

$$
b_{\sigma}= \begin{cases}\beta_{1}^{\sigma} & \sigma \in H \\ 1 & \sigma \notin H\end{cases}
$$

With the $d$-dimensional column vector $\boldsymbol{b}=$ $\left(b_{\sigma}\right)_{\sigma \in G} \in F_{1}^{d}$ and the regular matrix $W=\left(w_{\tau}^{\sigma}\right)$, we put

$$
\boldsymbol{t}=W^{-1} \boldsymbol{b}
$$

We claim that $\boldsymbol{t} \in k_{1}^{d}$. To see this, we write $\boldsymbol{t}=$ $\left({ }^{t} W W\right)^{-1}\left({ }^{t} W \boldsymbol{b}\right)$. It is well-known that the entries of ${ }^{t} W W$ belong to $k$. On the other hand, the entries of ${ }^{t} W \boldsymbol{b}$ belong to $k_{1}$, because

$$
\begin{aligned}
\sum_{\tau \in G} w_{\sigma}^{\tau} b_{\tau} & =\sum_{\tau \in H} w_{\sigma}^{\tau} \beta_{1}^{\tau}+\sum_{\tau \notin H} w_{\sigma}^{\tau} \\
& =\sum_{\tau \in H} w_{\sigma}^{\tau}\left(\beta_{1}^{\tau}-1\right)+\sum_{\tau \in G} w_{\sigma}^{\tau} \\
& =\operatorname{Tr}_{F_{1} / k_{1}}\left(w_{\sigma}\left(\beta_{1}-1\right)\right)+\operatorname{Tr}_{F / k}\left(w_{\sigma}\right)
\end{aligned}
$$

Now the relation $W \boldsymbol{t}=\boldsymbol{b}$ shows

$$
B_{\sigma}(\boldsymbol{t})=b_{\sigma} \neq 0 \quad(\sigma \in G)
$$

Moreover,

$$
A_{1}^{l}=\beta_{1}^{e(H)}=\prod_{\sigma \in H} \beta_{1}^{\sigma e_{\sigma}}=\prod_{\sigma \in G} b_{\sigma}^{e_{\sigma}}=\prod_{\sigma \in G} B_{\sigma}(\boldsymbol{t})^{e_{\sigma}}
$$

Then, by Lemma $2, \tilde{\gamma}_{\sigma}(\boldsymbol{t}) \neq 0$ and all the roots of $g(X ; \boldsymbol{t})$ are given by

$$
\theta_{j}=\sum_{\sigma \in G} \tilde{\gamma}_{\sigma}(\boldsymbol{t}) A_{1}^{x_{\sigma}} \zeta^{j \sigma}, \quad 0 \leq j \leq l-1
$$

Since $\tilde{\gamma}_{\sigma}(\boldsymbol{t}) \in F_{1}^{\times}$and $1, A_{1}, A_{1}^{2}, \ldots, A_{1}^{l-1}$ are linearly independent over $F_{1}$, we obtain $L_{1}=F_{1}\left(\theta_{j}\right)$, which yields

$$
\begin{aligned}
l=\left[L_{1}: F_{1}\right] & =\left[F_{1}\left(\theta_{j}\right): F_{1}\right] \\
& \leq\left[k_{1}\left(\theta_{j}\right): k_{1}\right] \leq \operatorname{deg} g(X ; \boldsymbol{t})=l
\end{aligned}
$$

and therefore $\left[k_{1}\left(\theta_{j}\right): k_{1}\right]=l$. Hence $K_{1}=k_{1}\left(\theta_{j}\right)$ for any $j$. This completes the proof.

Remark. If $H=G$, then it follows directly from Proposition 3 that $K_{1}$ is the splitting field of
$g(X ; \boldsymbol{t})$ over $k_{1}$ for some $\boldsymbol{t} \in k_{1}^{d}$, because $\left(w_{\sigma}\right)_{\sigma \in G}$ remains a basis of $F_{1}$ over $k_{1}$. So the essential difficulty of showing this fact in general is in the case where $H$ is a proper subgroup of $G$.

## References

[ 1 ] Cohen, H.: Advanced Topics in Computational Number Theory. Grad. Texts in Math., vol. 193, Springer, New York (2000).
[2] Dentzer, R.: Polynomials with cyclic Galois group. Comm. Algebra, 23, 1593-1603 (1995).
[ 3 ] Hashimoto, K., and Miyake, K.: Inverse Galois problem for dihedral groups. Number Theory and Its Applications (eds. Kanemitsu, S., and Gyory, K.). Developments in Math. vol. 2, Kluwer Academic Publ., Dordrecht, pp. 165-181 (1999).
[4] Saltman, D. J.: Generic Galois extensions and problems in field theory. Adv. Math., 43, 250283 (1982).
[5] Serre, J.-P.: Topics in Galois Theory. Jones and Bartlett Publ., Boston (1992).
[ 6 ] Smith, G. W.: Generic cyclic polynomials of odd degree. Comm. Algebra, 19, 3367-3391 (1991).


[^0]:    2000 Mathematics Subject Classification. 12F10, 12F12.

