PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 21 (35), 1977, pp, 197—200

UNIQUE FACTORIZATION IN GROUP-RINGS

Keng-Teh Tan

(Received June 11, 1976)

Abstract:

We show that the group-ring RG is a unique factorization domain iff R is and G is torsion-free abelian.

Terminologies undefined here will have the same meanings as in [1].

Let R be a principal ideal domain and $G=\langle x\rangle$ be the infinite cyclic group generated by x. Let $f\in RG$. Then we may write $f=x^m(a_0+\cdots+a_n x^n)$ for some $m\in\mathbf{Z}$, $n\geqslant 0$, $a_i\in R$. An element c of R is said to be a content of f if c is a greatest common divisor of $a_0, \ldots, a_n$. Cont (f) denotes the set of all contents of f. f is said to be primitive if the identity 1 of R is a g. c. d. of $a_0, \ldots, a_n$. Then we have the following

Lemma 1: *If $f, g\in RG$ are primitive, then so is fg.*

Proof: Write f as before and $g=x^l(b_0+\cdots+b_t x^t)$ for some $l\in\mathbf{Z}$, $t\geqslant 0$, $b_j\in R$. To show that fg is primitive, it suffices to show that $(a_0+\cdots+a_n x^n)\cdot(b_0+\cdots+b_t x^t)$ is primitive. But this can be proved in the same way as in Lemma 3.23, [1], page 120.

Proposition 2: *Let R be a* U. F. D., $G=\langle x\rangle$, $f, g\in RG$. *If* $\alpha\in\mathrm{Cont}(f)$, $\beta\in\mathrm{Cont}(g)$, *then* $\alpha\beta\in\mathrm{Cont}(fg)$.

Proof: Write $f=\alpha f_1$, $g=\beta g_1$ where $\alpha\in\mathrm{Cont}(f)$, $\beta\in\mathrm{Cont}(g)$, f_1, g_1 are primitive. Then

$$fg=\alpha\beta f_1 g_1.$$

Now $f_1 g_1$ is primitive. So $\alpha\beta\in\mathrm{Cont}(fg)$.

Lemma 3: *Let $G=\langle x\rangle$ be the infinite cyclic group and R a* U. F. D.: *with quotient field Q. Let $f\in R[x]$. Assume that f is both primitive and irreducible as an element of RG. Then f is irreducible as an element of QG.*

Proof: Assume f is not irreducible in QG. Since f is irreducible in RG $f\neq 0$ and $f\notin U(RG)$, the set of units in RG. So we may write $f=gh$, for some $g,\ h\in QG\backslash\{0\}$, $g,\ h\notin U(QG)$. Write $g=a^{-1}g_0$, $h=b^{-1}h_0$ for some $a,\ b\in R$, $g_0,\ h_0\in RQ$. Again, write $g_0=\alpha g_1$, $h_0=\beta h_1$, where $\alpha\in\mathrm{Cont}(g_0)$, $\beta\in\mathrm{Cont}(h_0)$ and both $g_1,\ h_1$ are primitive in RG. Thus, $f=gh=(a^{-1}b^{-1}\alpha\beta)g_1h_1$. So $(abf=(\alpha\beta)g_1h_1$. Now f and g_1h_1 are primitive, so ab and $\alpha\beta$ are associates. Hence $f=ug_1h_1$ for some $u\in U(R)$. This contradicts the irreducibility of f in RG.

Lemma 4: *Let R, G and Q be as before and $f\in RG$. Assume that f is primitive in RG and irreducible in QG then f is irreducible in RG.*

Proof: Trivial.

Lemma 5: *Let F be a field and $G=\langle x\rangle$. Then FG is a* P. I. D.

Proof: Clearly $F[x]\subseteq FG$. Also, for each $y\in FG$, $y=x^jf(x)$ for some $j\in\mathbf{Z}$ and $f(x)\in F[x]$.

Let A be a non-zero ideal of FG. We can pick a non-zero element $a(x)\in A\cap F[x]$ with minimal degree. We claim that $A=a(x)F(G)$. Clearly, $a(x)FG\subseteq A$. Next, let $y\in A$, $y\neq 0$. Write $y=x^jf(x)$ for some $j\in\mathbf{Z}$, $f(x)\in F[x]$. Then $f(x)\in A$. Also, $f(x)=q(x)a(x)+r(x)$ for some $q(x)$, $r(x)\in F[x]$ with $r(x)=0$ or $\deg(r(x)<\deg(a(x))$. Thus, $r(x)\in A\cap F[x]$. It follows that $r(x)=0$ by the minimality of $\deg(a(x))$. This shows that $f(x)\in a(x)FG$. Consequently, $y=x^jf(x)\in a(x)FG$. Hence $A\subseteq a(x)FG$. This proves Lemma 5.

Proposition 6: *Let R be a* U. F. D. *and $G=\langle x\rangle$. Then RG is a* U. F. D.

Proof: Trivially RG is an integral domain. Let Q be the quotient field of R. Then QG is a P. I. D. hence it is a U. F. D.

Let $p\in RG$ be primitive. Then as an element of QG, we can write $p=p\cdots p_k$, where each $p_i\in QG$ is irreducible. Write $p_i=a_i^{-1}f_i$ for some $a_i\in R$, $f_i\in RG$. Also, write $f_i=c_ig_i$, where $c_i\in\mathrm{Cont}(f_i)$ and g_i is primitive in RG. Then $p_i=a_i^{-1}c_ig_i$ since p_i is irreducible in QG, so g_i is irreducible in QG. Now by Lemma 4, g_i is irreducible in RG. Now,

$$p=p_1\cdots p_k=a_1^{-1}\cdots a_k^{-1}c_1\cdots c_kg_1\cdots g_k.\ \text{So}$$

$a_1\cdots a_kp_1\cdots p_k=c_1\cdots c_kg_1\cdots g_k$. Since $p_1\cdots p_k$ is primitive, so $a_1\cdots a_k\in\in\mathrm{Cont}(a_1\cdots a_kp_1\cdots p_k)$. Similarly, $c_1\cdots c_k\in\mathrm{Cont}(c_1\cdots c_kg_1\cdots g_k)$. Hence $p=p_1\cdots p_k=ug_1\cdots g_k$ for some $u\in U(R)$. This shows that every primitive element of RG is a product of irreducible elements in GR.

Next, assume that $p=r_1\cdots r_l$, where each $r_j\in RG$ is irreducible. Since p is primitive, so is each r_j. Hence each r_j is irreducible in QG. But QG is a U. F. D., so $l=k$ and for some $\sigma\in S_k$, r_j and $g_{\sigma(j)}$ are associates. This shows the unique factorization of primitive elements in RG.

Finally, let $f\in RG$ be arbitrary. Write $f=cf_1$, where $c\in\mathrm{Cont}(f)$ and $f_1\in RG$ is primitive. Thus, f_1 is a product of irreducible elements in RG. Also, since R is a U. F. D., c is a product of irreducible elements of R, hence also a product of irreducible elements of RG. It follows that f is a product of irreducible ele-

ments of RG. Now combining the unique factorization of f in the form cf_1 with $c \in R$, f_1 primitive and the unique factorization of c and of f_1, we have proved the Proposition.

Corollary: *Let R be a* U. F. D. *and G be a finitely generated torsion-free abelian group. Then RG is a* U. F. D.

Proof: Indeed, since G is finitely generated torsion-free abelian, then $G \cong c \times \cdots \times c_n$, where c_i is infinite cyclic. But then $RG \cong (Rc_1)(c_2 \times \cdots \times c_n)$, thus we may apply induction to complete the proof.

Lemma 7: *Let $f \in U(RG)$ and H be the support group of f. Then $f \in U(RH)$.*

Proof: Let $g \in RG$ be such that $fg = gf = 1$. Write $g = g_1 + g_2$ with $\mathrm{Supp}(g_1) \subseteq H$ and $\mathrm{Supp}(g_2) \cap H = \varnothing$. We note that for $a \in H$, $b \in G$, $ab \in H \Leftrightarrow$ $\Leftrightarrow b \in H$. Thus, from $fg = 1$, one has $fg_1 + fg_2 = 1$. Thus, it is clear $fg_2 = 0$. Hence $f \in U(RH)$.

Lemma 8: *Every torsion--free abelian group can be fully ordered.*

Proof: [2], Lemma 26.6, page 113.

We are now in a position to prove the following

Theorem: *RG is a* U. F. D. *iff R is a* U. F. D. *and G is torsion-free abelian.*

Proof. ($\Leftarrow$). Assume that R is a U. F. D. and G is torsion-free abelian. Let $0 \neq f \in RG$ and H the support group of f. Then H is finitely generated. Thus RH is a U. F. D. and $f \in RH$. Hence $f = f_1 \cdots f_n$ for some irreducible elements $f_i \in RH$. We claim that each f_i is also irreducible in RG. Indeed $f_i \neq 0$. Next, assume $f_i = \alpha\beta$ for some $\alpha, \beta \in RG \setminus \{0\}$ and $\alpha, \beta \notin U(RG)$. Let K be the subgroup of G generated by the supports of α and β. Let $H_i =$ supp. group of f_i. Then $H_i \subseteq K$. Also, K is finitely generated and $RH_i \subseteq RK$. Now RK is a U. F. D. and α, β, $f_i \in RK$. Hence either $\alpha \in U(RK) \subseteq U(RG)$ or $\beta \in U(RK) \subseteq$ $\subseteq U(RG)$, a contradiction. Hence f_i has no proper factorization in RG. Finally we observe that none of the f_i is invertible in RG, otherwise by Lemma 7, f_i would be invertible in RH, a contradiction. This proves the sufficiency of the theorem.

($\Rightarrow$). Assume that RG is a U. F. D. Then R is an integral domain and G is abelian. Next we show that G is torsion-free. Assume $g \in G$, $g \neq 1$, $g^n = 1$. Let $x = 1 + g + \cdots + g^{n-1}$ and $y = 1 - g$. Then $x \neq 0$, $y \neq 0$, but $xy = (1 + g + \cdots +$ $+ g^{n-1})(1 - g) = 0$, contradicting the assumption that RG is an integral domain. Hence G can be fully ordered by Lemma 8. Finally we show that R is a U. F. D. Let $0 \neq a \in R$, $a \notin U(R)$. Since RG is a U. F. D., $a = f_1 \cdots f_n$ for som irreducible elements f_i in RG. We claim that for each i, $f_i \in R$. Write

$$f_i = a_{i1} g_1^{(i)} + \cdots + a_{ij_i} g_{j_i}^{(i)}$$

with $g_1^{(i)} < \cdots < g_{j_i}^{(i)}$. If $j_i > 1$ for some i, then $f_1 \cdots f_n$ would contain at least two terms: $a_{11} \cdots a_{n1} g_1^{(1)} \cdots g_1^{(n)}$ and $a_{1j_1} \cdots a_{nj_n} g_{j_1}^{(1)} \cdots g_{j_n}^{(n)}$, a contradiction. Trivially, f_i is irreducible in R. Next, in view of the fact that the units of RG

are trivial (that is of the form ug for some $u \in U(R)$, $g \in R$), and the above proof, we note that an irreducible element of R is is also irreducible in RG. Thus the uniqueness of factorization in R follows from that in RG. This completes the prof of the theorem.

REFERENCES

[1] I. N. Herstein, *Topics in Algebra*, Blaisdell Publishing Co., 1964.
[2] D. S. Passman, *Infinite Group Rings*, Dekker, 1971.

Department of Mathematics
University of Malaya
Kuala Lumpur
Malaysia