Lie Regular Generators of General Linear Groups

Pramod Kanwar
Ohio University-Zanesville and Universitė d'Artois

Congress on Noncommutative Rings and their Applications

Lens, France
June 29-July 2, 2009

1 Background and Motivation

Definition 1 *An element a of a ring R is said to be unit regular if $a = aua$ for some unit u in R. Equivalently, a is unit regular if and only if $a = eu$ for some idempotent e and some unit u in R.*

Definition 2 *A ring R is called unit regular if each of its elements is unit regular.*

Definition 3 *An element $a \in R$ is called clean if $a = e + u$ for some idempotent e and some unit u in R.*

Definition 4 *A ring R is called clean if each of its elements is clean.*

Generalizations

- Strongly Clean,
- Uniquely Clean,
- 2-clean,
- n-clean, etc.

2 Definitions and Remarks

Definition 5 *An element a of a ring R is said to be* **Lie regular** *if $a = [e, u] = eu - ue$, where e is an idempotent in R and u is a unit of R. Further, a unit in R is said to be a* **Lie regular unit** *if it is Lie regular as an element of R.*

Example 1 *For any field F and $a \in F$, any matrix of the form $\begin{pmatrix} a & a \\ -a & -a \end{pmatrix}$ in $M_2(F)$ is a Lie regular element. For*

$$\begin{pmatrix} a & a \\ -a & -a \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & a \\ a & 1 \end{pmatrix} - \begin{pmatrix} 1 & a \\ a & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

if $a^2 \neq 1$. If $a^2 = 1$ then $a = 1$ or -1 and

$$\pm\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = \pm\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mp \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

Remark 1 *A ring in which all idempotents are central or a ring with no non trivial idempotents has no Lie regular elements. In particular, commutative rings, local rings, and reduced rings have no Lie regular elements.*

Remark 2 *Every Lie regular unit is unit regular. A Lie regular element need not be unit regular. A unit regular element need not be Lie regular.*

Example 2 *Let $R = \mathbb{Z}_2[S_3]$. Then $\tau + \sigma\tau$ is a Lie regular element but not a unit regular element.*

Nontrivial idempotents of $\mathbb{Z}_2[S_3]$ are

$$\{\alpha + \sigma^i + \sigma^{2j} \mid \alpha \in Z_2, 0 \leq i, j \leq 2, i \neq j\}$$

and

$$\{\alpha + \sigma^i + \sigma^j\tau + \sigma^k\tau \mid \alpha \in Z_2, 0 \leq i, j, k \leq 2, j \neq k\}.$$

Units in $\mathbb{Z}_2[S_3]$ are

$$\{\sigma^i\tau^j \mid 0 \leq i \leq 2, 0 \leq j \leq 1\},$$

$$\{1 + \sigma + \sigma^2 + \sigma^i\tau + \sigma^j\tau \mid 0 \leq i, j \leq 2, i \neq j\},$$

$$\{1 + \sigma^i + \tau + \sigma\tau + \sigma^2\tau \mid 0 < i \leq 2\},$$

and

$\{\sigma+\sigma^2+\tau+\sigma\tau+\sigma^2\tau\}$.

The element $\tau+\sigma\tau=[\sigma+\tau+\sigma\tau,\sigma]$ is a Lie regular element. It can be seen that $\tau+\sigma\tau$ is not a unit regular element.

Example 3 *If $\alpha\neq 0$ is an element in a field F, $u=\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}$ and $e=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$ then $a=eu=\begin{pmatrix}\alpha & 0\\ 0 & 0\end{pmatrix}$ is a unit regular element in $M_2(F)$ but it is not Lie regular.*

Remark 3 *The product of two Lie regular elements need not be Lie regular. Note that $u_1=\begin{pmatrix}0 & \alpha\\ 1 & 0\end{pmatrix}$ and $u_2=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ are both Lie regular units. However, the product $u_1u_2=\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}$ is not a Lie regular element if $\alpha\neq -1$.*

Remark 4 *If ϕ is an isomorphism from a ring R to a ring S and a is a Lie regular element (unit) in R then $\phi(a)$ is a Lie regular element (unit) in S.*

Proposition 4 *An element $a = (a_1, a_2, a_3, \ldots, a_n) \in R_1 \times R_2 \times R_3 \times ... \times R_n$ is a Lie regular element (unit) if and only if a_i is a Lie regular element (unit) for each i $(1 \leq i \leq n)$.*

Corollary 5 *If for some i, all idempotents in R_i are central then $R_1 \times R_2 \times R_3 \times ... \times R_n$ has no Lie regular units.*

Proposition 6 *If R has no Lie regular units then for any group G, the group ring RG has no Lie regular units.*

Proposition 7 *The inverse of a Lie regular unit in* $M_2(F)$ *is again Lie regular.*

Proof. If $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a Lie regular unit in $M_2(F)$ then $\alpha = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} = [e, u]$ and hence $\alpha^{-1} = [e, -\frac{1}{\det(\alpha)} u]$ which is lie regular. ∎

Remark 5 *If* $a = [e, u]$ *is a Lie regular unit then* $[1 - e, u]$ *is also a Lie regular unit.*

Remark 6 *If* $a = [e, u]$ *is a Lie regular unit then* $[e, u^{-1}]$ *is also a Lie regular unit. Note that* $[e, u^{-1}] = -u^{-1} a u^{-1}$.

Proposition 8 *No nonzero idempotent in a ring is Lie Regular.*

Proof. Suppose if possible, $e' = [e, u] = eu - ue$. Then $e'e + ee' = eu - ue = e'$. Also $ee'e = eue - eue = 0$. Thus, $(ee')^2 = 0 = (e'e)^2$. Now

$$\begin{aligned} e' &= e'^2 = (e'e + ee')^2 \\ &= (e'e)^2 + (ee')^2 + e'ee' + ee'e \\ &= e'ee'. \end{aligned}$$

Thus, $e' = e'^2 = e'ee'ee' = 0$. ∎

Proposition 9 *Let F be a finite field of q elements. If a is a Lie regular unit in $M_2(F)$ then $a^{2(q-1)} = I_2$, the 2×2 identity matrix.*

Lemma 10 *If R is a commutative domain then any non-trivial idempotent in $M_2(R)$ is of the form $\begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}$, $a(1-a) = bc$.*

Corollary 11 *If R is a commutative domain in which 2 is invertible then any idempotent in $M_2(R)$ is of the form $-I_2 + A$ where A is an invertible matrix in $M_2(R)$ and I_2 is the identity matrix.*

Corollary 12 *If R is a commutative domain in which 2 is invertible then any Lie regular element in $M_2(R)$ can be expressed as $[u_1, u_2]$ where u_1 and u_2 are invertible matrices in $M_2(R)$.*

Corollary 13 *If K is a field of characteristic different from 2 then any Lie regular element in $M_2(K)$ can be expressed as $[u_1, u_2]$ where u_1 and u_2 are invertible matrices in $M_2(K)$.*

Remark 7 *For any ring R and any $\lambda \in R$,* $\begin{pmatrix} 1 & \lambda \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ \lambda & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ \lambda & 1 \end{pmatrix}$, *and* $\begin{pmatrix} 0 & \lambda \\ 0 & 1 \end{pmatrix}$ *are idempotents in* $M_2(R)$.

Proposition 14 *If R is a commutative ring then any element in $M_2(R)$ of the form*

$$\begin{pmatrix} \lambda y & x \\ -y & -\lambda y \end{pmatrix}, \begin{pmatrix} -\lambda y & -y \\ x & \lambda y \end{pmatrix}, \begin{pmatrix} -\lambda y & y \\ -x & \lambda y \end{pmatrix}, \begin{pmatrix} \lambda y & -x \\ y & -\lambda y \end{pmatrix}$$

where λ, x, and y belong to R and xy is invertible in R, is a Lie regular element.

Proof. The proof is clear once we observe that

$$\begin{pmatrix} \lambda y & x \\ -y & -\lambda y \end{pmatrix} = \left[\begin{pmatrix} 1 & \lambda \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix} \right].$$

$$\begin{pmatrix} -\lambda y & -y \\ x & \lambda y \end{pmatrix} = \left[\begin{pmatrix} 0 & 0 \\ \lambda & 1 \end{pmatrix}, \begin{pmatrix} 0 & y \\ x & 0 \end{pmatrix} \right].$$

$$\begin{pmatrix} -\lambda y & y \\ -x & \lambda y \end{pmatrix} = \left[\begin{pmatrix} 1 & 0 \\ \lambda & 0 \end{pmatrix}, \begin{pmatrix} 0 & y \\ x & 0 \end{pmatrix} \right].$$

$$\begin{pmatrix} \lambda y & -x \\ y & -\lambda y \end{pmatrix} = \left[\begin{pmatrix} 0 & \lambda \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix} \right].$$

■

Corollary 15 *For any field F, any element in $M_2(F)$ of the form*

$$\begin{pmatrix} \lambda y & x \\ -y & -\lambda y \end{pmatrix}, \begin{pmatrix} -\lambda y & -y \\ x & \lambda y \end{pmatrix}, \begin{pmatrix} -\lambda y & y \\ -x & \lambda y \end{pmatrix}, \begin{pmatrix} \lambda y & -x \\ y & -\lambda y \end{pmatrix}$$

where λ, x, and y belong to F, is a Lie regular element.

Corollary 16 *Any matrix in $M_2(F)$ with trace 0 is Lie regular.*

Remark 8 *In general, the Lie product of Lie regular elements need to be Lie regular. The elements $x = \tau + \sigma\tau$ and $y = \sigma + \sigma^2 + \sigma\tau + \sigma^2\tau$ in $\mathbb{Z}_2[S_3]$ are both Lie regular. Their Lie product $[x, y] = \sigma + \sigma^2$ is, however, not Lie regular.*

Corollary 17 *Lie product of any two Lie regular elements in $M_2(F)$ is again a Lie regular element.*

Recall the infinite dihedral group D_∞, the group generated by two elements a and b where a is of infinite order and $b^2 = 1$, $ab = ba^{-1}$.

If K is a field of characteristic 2 then KD_∞ has no non-trivial idempotents and hence has no Lie regular elements.

Proposition 18 *If K is a field of characteristic different from 2 then every Lie regular element in KD_∞ can be written as $[u_1, u_2]$ where u_1 and u_2 are units in KD_∞.*

Proof. First observe that any element of KD_∞ can be written as $\alpha + b\beta$ where α and β belong to $K\langle a\rangle$. Also observe that for any Lie regular element the idempotent e in $[e, u]$ must be a nontrivial idempotent.

For any $\alpha = \sum \alpha_i a^i$ in $K\langle a \rangle$, let α^* denote the element $\sum \alpha_i a^{-i}$ in $K\langle a \rangle$. Since $ab = ba^{-1}$, it follows that $\alpha b = b\alpha^*$. We show that for every idempotent e in KD_∞, $e+1$ is a unit. So let $e = \alpha + b\beta$ be a nontrivial idempotent in KD_∞. Then $\alpha^2 + \beta\beta^* + b(\alpha^*\beta + \beta\alpha) = \alpha + b\beta$ and hence $\alpha^2 + \beta\beta^* = \alpha$ and $\alpha^*\beta + \beta\alpha = \beta$. If $\beta = 0$ then $\alpha^2 = \alpha$. Since $K\langle a \rangle$ is a domain, it follows that α is 0 or 1, a contradiction. Thus $\beta \neq 0$. Invoking once again the fact that $K\langle a \rangle$ is a domain $\alpha^*\beta + \beta\alpha = \beta$ gives $\alpha + \alpha^* = 1$. Since $\alpha^2 + \beta\beta^* = \alpha$ we get $\beta\beta^* = \alpha - \alpha^2 = \alpha\alpha^*$. But then $[(\alpha + 1) + b\beta]\left[\frac{(\alpha^* + 1)}{2} - b\frac{\beta}{2}\right] = 1$. It follows that $e + 1 = (\alpha + 1) + b\beta$ is a unit in KD_∞. In other words, every idempotent in KD_∞ can be expressed as $u - 1$ for some unit u in KD_∞. ■

Remark 9 *In general Lie regular elements need not be of the form $[u_1, u_2]$ where u_1 and u_2 are units. Consider $\mathbb{Z}_2[S_3]$. The Lie regular element $\sigma + \sigma^2 + \sigma\tau + \sigma^2\tau$ is not a Lie product of two units.*

3 Lie Regular Generators of General Linear Groups

Theorem 19 *Let F be the finite field with p elements, that is, $F = \mathbb{Z}_p$. The unit group of $M_2(F)$ is generated by Lie regular units a, b, and c where $a = \begin{pmatrix} 0 & 1 \\ \alpha & 0 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$, $c = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, where α is a primitive root modulo p. Indeed, the unit group of $M_2(F)$ is the group*

$$\begin{aligned}\langle a, b, c \,|\, & c^2, (ca)^{p-1}, (ca)^{(p-1)/2}(ca^{p-1})^3 c, (c(ca^{p-1})^{-1}b)^p, \\ & (ca)^{-1}(c(ca^{p-1})^{-1}b)(ca) = (c(ca^{p-1})^{-1}b)^{\alpha}, \\ & (ca)^{-1}(ca^{p-1})ca = (ca^{p-1})(c(ca^{p-1})^{-1}b)^{1/\alpha} \\ & (ca^{p-1})(c(ca^{p-1})^{-1}b)^{\alpha}(ca^{p-1})(c(ca^{p-1})^{-1}b)^{1/\alpha} \\ & (ca^{p-1}), (ca^{p-1})^2 = (c(ca^{p-1})^{-1}b(ca^{p-1}))^3 = \\ & ((c(ca^{p-1})^{-1}b)^4(ca^{p-1})(c(ca^{p-1})^{-1}b)^{(p+1)/2}(ca^{p-1}))^2\rangle\end{aligned}$$

Proposition 20 *For any prime p, the order of the linear group $GL(2, \mathbb{Z}_{p^n})$ is $p^{2n-1}(p+1)(\phi(p^n))^2$.*

Proof. Use order of $GL(2, \mathbb{Z}_p)$ is $p(p+1)(p-1)^2$. and the surjective homomorphism $\sigma : GL(2, \mathbb{Z}_{p^n}) \to GL(2, \mathbb{Z}_p)$ ■

Corollary 21 *For any prime p, the order of $SL(2, \mathbb{Z}_{p^n})$ is $p^{2n-1}(p+1)\phi(p^n)$.*

Proposition 22 *If p is an odd prime then the order of $GL(2, \mathbb{Z}_{2p})$ is $6p(p+1)\phi(2p)^2$.*

Proof. Use $GL(2, \mathbb{Z}_{2p}) \cong GL(2, \mathbb{Z}_2) \times GL(2, \mathbb{Z}_p)$ ■

Corollary 23 *If p is an odd prime then the order of $SL(2, \mathbb{Z}_{2p})$ is $6p(p+1)\phi(2p)$.*

Theorem 24 *Let p be an odd prime and $\alpha \neq 2$ be a primitive element modulo p. Then $GL(2, \mathbb{Z}_{2p})$ is generated by $a = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $c = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix}$.*

Theorem 25 *If $n > 2$ then $GL(2, \mathbb{Z}_{2^n})$ is generated by $a = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $c = \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix}$, and $d = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.*

Theorem 26 *If p is an odd prime then $GL(2, \mathbb{Z}_{p^n})$ is generated by $a = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and $c = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix}$ where α is a primitive element modulo p^n.*

Theorem 27 *If p is an odd prime then $GL(2, \mathbb{Z}_{2p^n})$ is generated by $a = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and $c = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix}$ where $\alpha \neq 2$ is a primitive element modulo p^n.*

Theorem 28 $GL(2,\mathbb{Z}_4) = \langle a, b, c \,|\, a^2, b^2, c^4, c^2a = ac^2, c^2b = bc^2, bc = c^{-1}b, (ab)^3, (cba)^4\rangle$, *where* $a = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ *and* $c = \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix}$.

Theorem 29 *The group* $GL(2,\mathbb{Z}_6)$ *is generated by* $a = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, *and* $c = \begin{pmatrix} 0 & 5 \\ 1 & 0 \end{pmatrix}$. *The relators on the generators are* $a^2, b^2, c^4, c^2b = bc^2, c^2a = ac^2, (ab)^3, (bc)^2, (ac)^{12} = c^2, (ca)^2b(ca)^2 = (ac)^2b(ac)^2$. *In other words,*

$$\begin{aligned} GL(2,\mathbb{Z}_6) = \langle a, b, c \,|\, & a^2, b^2, c^4, c^2b = bc^2, c^2a = ac^2, \\ & (ab)^3, (bc)^2, (ac)^{12} = c^2, \\ & (ca)^2b(ca)^2 = (ac)^2b(ac)^2\rangle \end{aligned} .$$

Theorem 30 *The group $GL(2,\mathbb{Z}_8)$ is generated by* $a = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $c = \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix}$, *and* $d = \begin{pmatrix} 0 & 7 \\ 1 & 0 \end{pmatrix}$. *Indeed,*

$$\begin{array}{rl} GL(2,\mathbb{Z}_8) = \langle a,b,c,d \,|\, & a^2, b^2, c^4, d^4, c^2a = ac^2, \\ & c^2b = bc^2, c^2d = dc^2, d^2a = ad^2, d^2b = bd^2, \\ & d^2c = cd^2, (ab)^3, (bc)^2, (bd)^2, (cd)^2, (ac)^6, \\ & c(ad)^2 = ba(ca)^2bc^3a, (ad)^6, (dab)^8\rangle, \end{array} .$$

Theorem 31 *The group $GL(2,\mathbb{Z}_{10})$ is generated by* $a = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, *and* $c = \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix}$. *Indeed,*

$$\begin{array}{rl} GL(2,\mathbb{Z}_{10}) = \langle a,b,c \,|\, & a^2, b^2, c^8, c^2b = bc^2, c^2a = ac^2, \\ & (ab)^3, (bc)^4, bca(cb)^2ab = cab(ac)^2\rangle \end{array} .$$

Thank You