مجلة جامعة تشرين للبحوث والدراسات العلمية – سلسلة العلوم الأساسية المجلد (32) العدد (1) 2010
Tishreen University Journal for Research and Scientific Studies - Basic Sciences Series Vol. (32) No. (1) 2010

البيانات التامة الموجهة الدورية من المرتبة p^q حيث P, q عددان أوليان

الدكتور اسكندر علي*

(تاريخ الإيداع 5 / 11 / 2009. قُبِل للنشر في 10 / 2 /2010)

□ ملخّص □

استعرضت في هذا البحث الزمرة التآلفية الخطية:

$$\Phi = \{x \longmapsto a\sigma(x) + b\,, a \neq 0, b, x \in GF\,(p^q), \sigma \in Aut\; GF(p^q)\}$$

وقد برهنت أنه يوجد في هذه الزمرة فقط زمرة جزئية عظمى وحيدة ذات رتبة فردية، وحددت الشروط اللازمة الكافية لوجود زمرة جزئية ابتدائية في الزمرة التآلفية الخطية، وبموجب ذلك تم بناء جميع البيانات التامة الموجهة التي تقبل الزمرة الجزئية العظمى المذكورة آنفاً كزمرة أوتومورفيزمز.

تدعى هذه البيانات التامة الموجهة بالبيانات التامة الدورية.

الكلمات المفتاحية: زمرة ابتدائية، بيان تام موجه، بيان تام دوري

* أستاذ– قسم الرياضيات– كلية العلوم– جامعة تشرين – اللاذقية –سورية.

مجلة جامعة تشرين للبحوث والدراسات العلمية – سلسلة العلوم الأساسية المجلد (32) العدد (1) 2010
Tishreen University Journal for Research and Scientific Studies - Basic Sciences Series Vol. (32) No. (1) 2010

Cyclotomic Data of Order p^q , where p, q Primes

Dr. Eskandar Ali*

(Received 5 / 11 / 2009. Accepted 10 / 2 /2010)

□ ABSTRACT □

We take the linear affine group:

$\Phi = \{x \mapsto a\sigma(x) + b\,, a \neq 0, b, x \in GF\,(p^q), \sigma \in Aut\ GF(p^q)\}$

and we consider the odd order subgroups of the linear affine. We show that it has a unique maximal odd order subgroup and we determine all of the primitive subgroups of the linear affine group, so that we construct the data admitting this subgroup as an automorphism group. We call these data Cyclotomic data.

Keywords: Primitive Group, Tournaments, Cyclomatic Tournaments.

* **professor , department of mathematics, Faculty of science, Tishreen university, Lattkai, Syria**

مقدمة:

تعدّ زمر الأوتومرفيزم للبيانات أداة مهمة في توزيع البيانات إلى صفوف غير متماثلة.

فإذا كانت G زمرة تباديل معطاة فإن المطلوب هو بناء البيانات– إن وجدت–التي تمثل G زمرة أوتومرفيزم لها وهذه المسألة معروفه بمسألة(Kunek) وأحد مناحيها المسألة المفتوحة الآتية:

لتكن G زمرة جزئية متعدية (transitive) في زمرة التباديل والمطلوب بناء البيانات التامة الموجهة– إن وجدت– بحيث تكون G هي زمرة الأوتومرفيزم لكل منها.

أهمية البحث وأهدافه:

إن أهمية البحث تكمن في تصنيف البيانات التامة الموجهة من خلال استخدام زمرة الأوتومورفيزم ومعلوم أن علم الزمر متقدم جداً على علم البيانات

طرائق البحث ومواده:

استخدمت المقالات ذات الصلة والمراجع المناسبة

ومما هو جدير بالذكر أنه ليست جميع الزمر المتعدية هي زمرأوتومرفيزم لبيانات تامة موجهة وفي هذا السياق برهن الباحثان(Babai-Imrch)[7]أنه لأجل الزمرة المتعدية G التي تكون زمرتها المثبتة هي الواحدة {e} لايوجد بيانات تامة موجهة Tبحيث إن G=Aut(T) باستثناء الحالة: $G=Z_3 \times Z_3$.

مصطلحات وتعاريف:

1) S(X) زمرة التباديل على X (Permutation group)

2) $GF(p^q)$ حقل منتهي مؤلف من p^q عنصر حيث p,q عددان أوليان ويمكن النظرإلى $GF(p^q)$ كتوسيع بسيط للحقل البسيط $GF(p)$، وعليه فإنه يمكننا النظر إلى الحقل المنته $GF(p^q)$ كفضاء من المتجهات معرف على $GF(p)$ بحيث إنه إذا كان ω عنصراًإبتدائياً فيه فإن مجموعة العناصر $\{1, \omega, \omega^2, \ldots . \omega^{q-1}\}$ تشكل قاعدة للفضاء $GF(p^q)$ المعرف على الحقل $GF(p)$.

3) GL(q,p) الزمرة الخطية العامة (General linear group) التي عناصرها مصفوفات مربعة نظامية معرفة على $GF(p)$ ودرجتها q.

4) ((Aut($GF(p^q)$ زمرة الأوتومرفيزم على الفضاء $GF(p^q)$ بالنسبة لـ $GF(p)$ حيث إن الزمرة Aut($GF(p^q)$)) تثبت عناصر الحقل الجزئي $GF(p)$.

5) تعريف: يسمى البيان الذي يوجد بين كل رأسين مختلفين فيه ضلع موجه واحد فقط بيان تام موجه (tournament) .

نرمز للبيان التام الموجه بالرمز T=(X,U) حيث: X مجموعة رؤوسه (vertices)

U مجموعة أضلاعه (arcs)

إذا كانت x،y عقدتين من X سنرمز للضلع الموجهة من العقدة x إلى العقدة y بالرمز $\exists$(x,y) U

6) Aut(T)– زمرة الأوتومورفيزم للبيان التام الموجه، وهي مجموعة العناصر f من S(X) التي تحافظ على تجاور أضلاع البيان T :

$$\forall f \in Aut\,T, \forall (x,y) \in U \Rightarrow (f(x), f(y)) \in U$$

مبرهنة (1):

(i) إذا كانت G زمرة جزئية في الزمرة التآلفية الخطية المؤلفة من جميع التحويلات الآتية

$$\Phi = \{x \mapsto a\sigma(x) + b\,, a \neq 0, b, x \in GF\,(p^q), \sigma \in Aut\,GF(p^q)\}$$

حيث p, q عددان أوليان.

فإن الشرط اللازم الكافي لكي تكون G إبتدائية (primitive)هو أن لاتكون رتبة G_0 قاسماً للعدد p-1 حيث إن G_0 هي الزمرة الجزئية المثبتة للصفر في G.

(ii) إذا كانت G' زمرة جزئية في الزمرة الآتية:

$$\Phi' = \{x \mapsto ax + b\,, a \neq 0, b, x \in GF\,(p^q) \quad .$$

فإن الشرط اللازم الكافي لكي تكون G' إبتدائية هوأن لا تكون رتبة G'_0 قاسماً للعدد p-1حيث إن G'_0هي الزمرة الجزئية المثبتة للصفر في G' .

(iii) إذا كانت K'_0 زمرة جزئية في الزمرة المثبتة Φ'_0 حيث :

$$\Phi'_0 = \{x \mapsto ax\,, a \neq 0, x \in GF(p^q)\}$$

بحيث إنK'_0 تحقق ما يأتي: 1) غير خزولة(irreducible) على $GF(p^q)$.

2) $q \nmid |K'_0|$

عند ئذٍ تكون K'_0 إبتدائية .

البرهان:نبرهن أولاً(ii)،معلوم من نتائج [8] أن الشرط اللازم الكافي لكي تكون الزمرة G' إبتدائية هو أن تكون الزمرة المثبتة G'_0 غير خزولة على $GF\,(p^q)$ وبما أن G' زمرة جزئية في Φ' إذن يكون لِـ G' الشكل الآتي :

$$G' = \{X \mapsto a^l x + b\ ;\ a \neq 0,\ b, x \in GF(p^q); l \mid (p^q - 1)\}$$

فإن للزمرة المثبتة للصفر الشكل الآتي [1]:

$$G'_0 = \{X \mapsto a^l x\ ;\ a \neq 0,\ x \in GF(p^q); l \mid (p^q - 1)\}$$

فإذا كانت G'_0 خزولة(reducible)على $GF\,(p^q)$ (كفضاء متجهات معرف على $GF\,(p)$) فإن أي فضاء جزئي في $GF\,(p^q)$ يكون مستقراً بالنسبة لِـ G'_0 [4] وعليه فإن:

$$G'_0(GF(p)) = GF(p) \Rightarrow$$

$$\Rightarrow \forall\, g' \in G'_0,\ x \in GF(p)^*: g'(x) = a^l x \in GF(P)^* \Rightarrow \quad \forall$$

$$\Rightarrow a^l \in GF(P)^* \Rightarrow < a^l > \subseteq GF(P)^* \Rightarrow |G_0| \mid (p-1)$$

العكس: نفرض أن $|G'_0| \mid (p-1)$ ، سنبرهن أن G'_0 خزولة على $GF(p^q)$

بما أن$G'_0 = \{x \mapsto a^l x\ ;\ \ a \neq 0,, x \in GF\,(p^q)\}$

حيث $(p^q - 1) \mid l$ وبما أن $|G'_0| \mid (p^q - 1)$ إذ ن $a^l \in GF(P)^*$

وبالتالي فإن $G_0' \subseteq GF(P)^*$ وينتج من ذلك أن : $G_0'(GF(p)) = GF(p)$

وبما أن $GF(p)$ هو الفضاء الجزئي الخاص الوحيد في الفضاء $GF(p^q)$ فهذا يعني أ ن جميع الفضاءات الجزئية مستقرة بالنسبة لِ G_0'، وعليه فإن G_0' خزولة على$GF(p^q)$،مما تقدم نجد أن الشرط اللازم الكافي لتكون G_0' غير خزولة (irreducible)هو أن لا يكون العدد $|G_0'|$ قاسماً للعدد p-1.

(i) يتم البرهان على (i) بالطريقة السابقة نفسها.

(iii) نفرض جدلاً أن K_0' غير ابتدائية عند ئذ توجد جملة لا إبتدائية $\{V_\alpha, \alpha \in I\}$ من الفضاءات الجزئية في الفضاء$GF(p^q)$ المعرف على $GF(p)$ بحيث إن:

$$GF(p^q) = \cup_{\alpha \in I} V_\alpha \; ; \quad V_i \cap V_j = \{0\}, \forall\, i \neq j$$

نلاحظ أنه لا يوجد في الجملة $\{V_\alpha, \alpha \in I\}$ عنصر مستقر بالنسبة إلى الزمرة الجزئية K_0' (لأن K_0'غير خزولة)، وعليه فإن K_0' تجري مناقلة بين الفضاءات الجزئية في الجملة$\{V_\alpha, \alpha \in I\}$ كزمرة متعدية [5] فإن عدد أبعاد هذه الفضاءات الجزئية متساوية وكل منها يساوي الواحد

(لأن $\dim V_\alpha$ يقسم العدد الأولي q).

إذن مما تقدم نجد أن :

$$q=\dim\ GF(p^q) = \Sigma_{\alpha \in I} \dim V_\alpha = \sum_{\alpha=1}^{q} \dim V_\alpha$$

حيث إن$\dim V_\alpha$=1 لكل $\alpha \in I$ وعليه فإن $I=\{1,2,3,\ldots\ldots\ldots\ldots,q\}$ و معلوم من علاقة (Burnside) [8] أن طول المدار للزمرة K_0' يقسم الرتبة $|K_0'|$ وعليه فإن طول المدار I يقسم $|K_0'|$ إذن $|K_0'|$ | q ، وهذا يناقض الفرض. إذاً الفرض الجدلي غير صحيح وينتج من ذلك أن K_0' ابتدائية .

□ إذا كان n عدداً طبيعياً وكان ξ عدداً أولياً بحيث إن $\xi|n$ وإذا قسمنا n على ξ عدداً من المرات $v_\xi(n)$حتى نحصل على ناتج قسمة صحيح m بحيث إن $\xi \nmid m$ ، سندعو العدد $v_\xi(n)$ بأعلى قوة للعامل الأولي ξ في تحليل n إلى عوامله الأولية ويكون :

$$n=\xi^{v_\xi(n)}.\, m \quad ; \quad \xi \nmid m$$

مبرهنة (2): ليكن p,q عددين أوليين ولتكن G زمرة جزئية في الزمرة التآلفية الخطية Φ مؤلفة من التحويلات الآتية [2]:

$$G = \{x \longmapsto a^{2^{v_2(p^q-1)}} \sigma^{2^{v_2(q)}}(x) + b\,, a \neq 0, b, x \in GF\,(p^q)\,,\ \sigma \in Aut\ GF(p^q)\}$$

حيث $v_2(q)$ و $v_2(p^q-1)$ أعلى قوة للعامل الأولي 2 في تحليل q و p^q-1 إلى الشكل القانوني على الترتيب. عندئذ ما يأتي صحيح:

(i) الزمرة G عظمى في مجموعة الزمر الجزئية ذوات الرتب الفردية في Φ.

(ii) الزمرة $\Phi_0 = \{x \longmapsto ax^{p^i}; 0 \neq a \in GF(p^q), i = 0,1,\ldots.,q-1\}$ عظمى في مجموعة الزمر الإبتدائية القابلة للحل الجزئية في الزمرة $GL(q,p)$.

البرهان: واضح أن $|G| = p^q \frac{p^q-1}{2^{v_2(p^q-1)}} \frac{q}{2^{v_2(q)}}$ عدد طبيعي فردي .

ولبرهان(i) يكفي أن نبرهن أنه إذا كان g عنصراً اختيارياً من Φ وكان $|g|$ عدداً فردياً فإن $g\in G_0$ (حيث G_0 هي الزمرة الجزئية المثبتة للصفر في G).

نفرض أن $|g|=\propto$ حيث $\propto$ عدد طبيعي فردي ولنفرض w عنصراً إبتدائياً في $GF(p^q)^*$. بما أن $g\in\Phi$ إذن يوجد عدد صحيح l : $1\le l\le p^q-1$ ويوجد عدد صحيح j: $1\le j\le q-1$ بحيث تتحقق العلاقة الآتية :

$$\forall x\in GF(p^q): g(x)=w^l x^{p^j}\Rightarrow g^{\propto}(x)=w^{l(1+p^j+\cdots+p^{j(\propto-1)})}x^{p^{j\propto}}$$

وبما أن $\propto$ رتبة g إذن $g^{\propto}(x)=x$ لكل x ∋ $GF(p^q)$ وعليه فإن :

$$W^{l(1+p^j+\ldots+p^{j(\alpha-1)}q)}=1=W^{p^q-1}\ \&\ p^{j\alpha}=p^q\Rightarrow$$

$$\Rightarrow l(1+p^j+\ldots+p^{j(\alpha-1)})\mid(p^q-1)\Rightarrow l\mid 2^{v_2(p^q-1)}$$

لأن ($1+p^j+\cdots.+p^{j(\propto-1)}$)عدد فردي وعليه فإن $l=2^s$ حيث s عدد صحيح ≤ 1

وبالتالي فإن: $g(x)=w^{2^s}x^{p^j}$ وهذا ما يبرهن أن $g\in G_0$.

(ii) نرمز $\overline{G}$ للزمرة العظمى في مجموعة الزمرالجزئية الابتدائية القابلة للحل في *GL(q,p)* وسنبرهن أن $\overline{G}=\left\{x\mapsto ax^{p^i};a\neq 0,x\in GF(p^q),i=1,\ldots,q-1\right\}$:

بما أن $\overline{G}$ إبتدائية إذن توجد فيها زمرة جزئية إبدالية نظامية عظمى D [6] وإذا اعتبرنا $GF(p^q)$ فضاء متجهات على *GF(p)* فيمكن تمثيل D بالتحويلات التالية:

$D=\{x\mapsto ax\ ;\ a\neq 0,x\in GF(p^q)$ (لأن عناصر D مؤلفة من مصفوفات قطرية)

ولنرمز لزمرتي المنظم والممركز للزمرة D في *GL(q,p)* بالرمزين: *N(D), C(D)* على الترتيب ولنعرف التطبيق φ كما يلي [3] :

$$\varphi: N(D)\to\overline{G}\quad :\ g\to\bar{g}\ ,\ \forall g\in N(D)$$

حيث: $\bar{g}: GF(p^q)\to Aut\ GF(p^q): x\mapsto x^{-1}gx\ ,\forall x\in GF(p^q)$

من السهل التحقق أن φ هومرفيزم غامر [5].

واضح أن $\overline{G}\le N(D)$ وأن $ker\ \varphi=C(D)$ وعليه فإن :

$$N(D)\ /\ C(D)\cong Aut\ GF(p^q)$$

وبما أن $(GF(p^q):GF(p))=q$ إذن $D=C(D)$ & $Aut\ GF(p^q)$ زمرة دورية رتبتها q.

وعليه فإن :

$$N(D)\ /\ D\cong Aut\ GF(p^q)$$ وبالتالي :

$$|N(D)|=|D|\ |Aut\ GF(p^q)|$$.

أو $|N(D)|=(p^q-1)q$ (1)

ومن السهل التحقق أيضا أنه لكل $g\in\Phi_0$ يكون $gDg^{-1}=D$ وعليه فإن $\Phi_0\subseteq N(D)$

وإذا لاحظنا أن رتبة Φ_0 (بحسب تعريف Φ_0) تعطى بالعلاقة: $|\Phi_0|=(p^q-1)q$

سنجد من المساواة (1) أن $\Phi_0=N(D)$.

وبما أن $\overline{G} \subseteq N(D)$ إذن $N(D)$ إبتدائية (لأن $\overline{G}$ إبتدائية) وفوق ذلك نرى بوضوح أن $N(D)$ قابلة للحل لأنها تحوي سلسلة نظامية $\{e\}\triangleleft D\triangleleft N(D)$ (لأن $|N(D)/D| = q$ حيث q عدد أولي وبالتالي فإن $N(D)/D$ إبدالية) .

وهكذا وجدنا أن $N(D)$ زمرة ابتدائية قابلة للحل تحوي $\overline{G}$ ولكن $\overline{G}$ عظمى في مجموعة الزمر الإبتدائية القابلة للحل في $GL(q,p)$ وعليه فإن $\overline{G} = N(D)$ وينتج من ذلك أن:

$$\overline{G} = N(D) = \Phi_0 = \left\{x \mapsto ax^{p^i}; a \neq 0, x \in GF(p^q), i = 0,1,\dots,q-1\right\}$$

لنأخذ الزمرة الجدائية $GF(p^q)^*$في الحقل $GF(p^q)$ ولنكتب :

p,q عددان أوليان ولنأخذ في $GF(p^q)^*$ الزمرة الجزئية H التي $p^q - 1 = 2^{v_2(p^q-1)}\ h$ حيث

رتبتها h فتكون:$H =< a^{2^{v_2(p^q-1)}}; a \neq 0 \in GF(p^q) >$

نلاحظ أن الزمر العاملة $GF(p^q)^*/H$ تحوي $2^{v_2(p^q-1)}$ صف مجاورللزمرة H تسمى هذه الصفوف بصفوف دورية في الحقل $GF(p^q)$.

وبما أن h عدد فردي إذن $xH \neq -xH$ لكل x من $GF(p^q)$ [2] وبالتالي نحصل على التجزئة الآتية للزمرة $GF(p^q)^*$:

$$GF(p^q)^* = x_1H \cup (-x_1)H \cup \dots \cup x_kH \cup (-x_k)H\,;\, k = \frac{1}{2}(2^{v_2(p^q-1)})$$

ولنعرف البيان التام الموجه الدوري وبالإستفادة من الزمرة H كمايلي:

$$T = (X,U): \left\{\begin{array}{l} X = GF(p^q) \\ (x,y) \in U \Leftrightarrow y - x \in S = \bigcup_{i=1}^{k} \mathcal{E}_i x_i H \end{array}\right\} \qquad (1)$$

حيث $\mathcal{E}_i = \pm 1$ لكل $i=1,2,\dots,k$

نلاحظ أن S هي اجتماع k صف دوري يتم اختيارهم من $2k$ صف دوري بحيث إذا دخل الصف xH في S فلا يدخل الصف$(-x)H$ في S وبالعكس .

واضح أنه يوجد 2^k إمكانية لتعريف بيان تام موجه بدلالة S ، نرمز للبيان T المعرف بدلالة S بالرمز $T(S)$.

واضح أن البيان التام الموجه الدوري $T(S)$ *(cyclotomic)* المعرف في (1) يخضع في تعريفه لطريقة بناء المجموعة S .

مثال:بفرض $p=5,q=2$ والمطلوب بناء $GF(p^q)^*$ عندما $p=5, q=2$

الحل:لدينا في الحقل $GF(p^q)$ العلاقة الآتية: $\forall x \in GF(p)^* \ : x^{p^q} = x$

وبالتالي فإن : $\forall x \in GF(p)^* \ : x^{p^q-1} = 1$

وفي مثالنا نقوم بتحليل $x^{24}-1$ إلى عوامل أمثالها من الحقل $GF(5)$ حتى نحصل على كثير الحدود الأصغري $m(x)$ فنجد أن :

$$x^{24} - 1 = (x^{12}-1)(x^6-2)(x^2+3)(x^4+2x^2+4) = 0$$

ويكون كثير الحدود الأصغري: $m(x) = x^4 + 2x^2 + 4$.

ومن السهل ملاحظة أن $w=\sqrt{3}-1$ جذرٌ لـ $m(x)$ وبالتالي يكون $GF(5^2)^* =< w >$

وبترتيب عناصر $GF(p^q)^*$ حسب قوى w نحصل على :

$w, w^2, w^3, \dots, w^{23}, w^{24} = 1$ وتكون إحداثيات هذه المتجهات في القاعدة $\{1, w\}$ هي على الترتيب :

$$w=(0,1)\ , w^2 = (2,2)\ , w^3 = (-1,1)\ , w^4 = (2,1)\ , w^5 = (2,-1),$$
$$w^6 = (-2,0),\ w^7 = (0,-2)\ , w^8 = (1,1)\ , w^9 = (2,-2),$$
$$w^{10} = (1,-2), w^{11} = (1,2), w^{12} = (-1,0),$$
$$w^{13} = -w = (0,-1), w^{14} = -w^2 = (-2,2), \dots\dots\dots\dots,$$
$$w^{23} = -w^{11} = (-1,-2), w^{24} = (1,0) \quad ,\dots\dots,$$

ونلاحظ أن : $p^2 - 1 = 5^2 - 1 = 2^3.3$ وعليه فإن : $v_2(2) = 3$ وتكون الزمرة الجزئية H:

$H = < w^{2^3} > = \{w^8, w^{16}, 1\}$

وعليه فان الصفوف الدورية في $GF(5^2)$ بالنسبة إلى الزمرة H هي :

$H, wH, \dots\dots, w^7 H$

يتم تشكيل المجموعة S من k إجتماع صف دوري (في مثالنا $k=4$) بحيث إذا دخل في S الصف الدوري $w^i H$ فلا يدخل فيها $(-w^i)H$ وبما أن عدد طرائق اختيار k صف من $2k$ صف يتم بـ 2^k طريقة إذن توجد 2^k مجموعة S وبالتالي يوجد 2^k بيان تام موجه دوري $T(S)$. على سبيل المثال نشكل المجموعة S كالتالي :

$$S = H \cup w^2 H \cup (-w)H \cup (-w^3)H =$$
$$= \{(1,1), (-2,-1), (1,0), (-2,2), (2,-1), (-1,0), (1,-2), (2,0),$$
$$(2,2), (-1,-2), (0,-2), (1,-1)\}$$

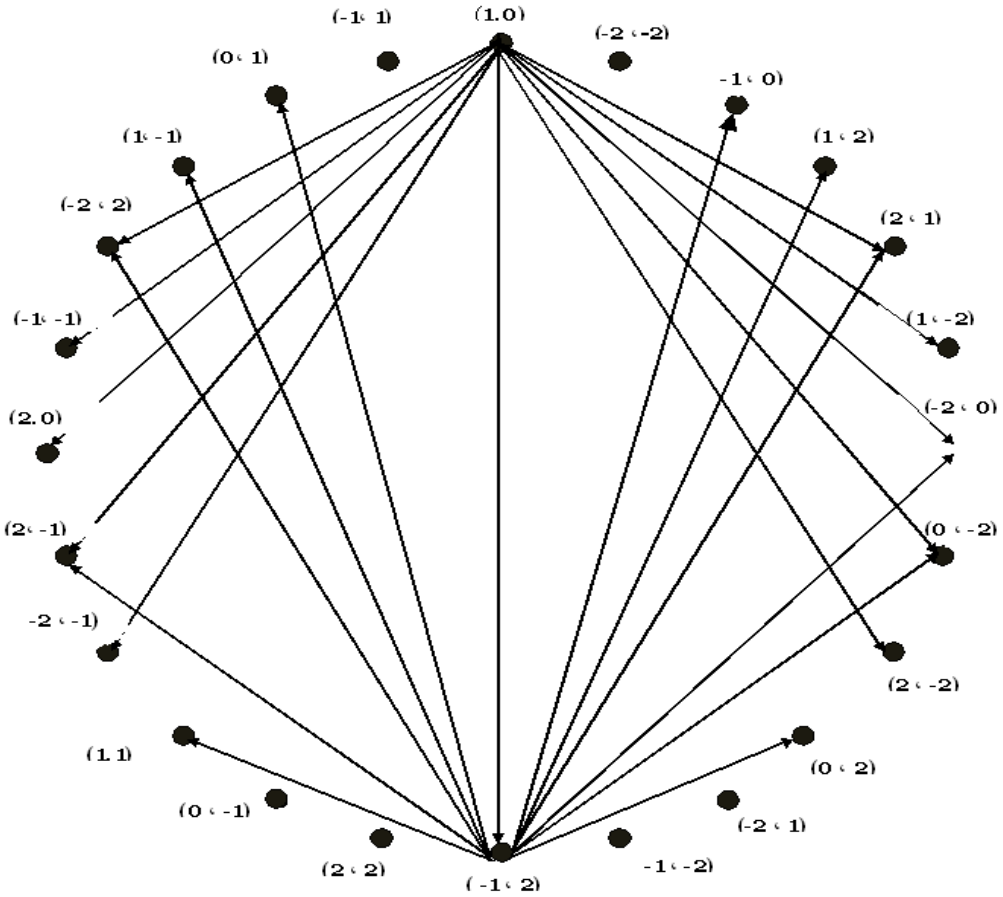
ويتم رسم البيان التام الموجه الدوري (*Cyclotomic*) الآتي : $T(S) = (GF(p^q), U)$

وفق القاعدة التالية: $\forall\ x, y \in GF(p^q)\ :\ (x,y) \in U \Leftrightarrow y - x \in S$

مثلاً : $((2\ ,\ 2)\ ,\ (0\ ,\ 1)) \in U$ لأن $(0\ ,\ 1) - (2,\ 1) = (-2\ ,-1) \in U$

وهكذا يتم توجيه أي ضلع من U .

ونكتفي برسم جزء *من البيان* $T(S)$ كما يلي (للتوضيح فقط) :



نظرية : ليكن $T=(X,U)$ بياناً تاماً موجهاً دورياً رتبته P^q حيث p و q عددان أوليان وبحيث إنه عندما يكون q=2 فإن $P+1\neq 2^S$ حيث s عدد صحيح ≥ 1 ولنرمز لزمرة الأوتومورفيزم للبيان T بالرمز $A(T)=Aut\ T$ ولنرمز بـ G للزمرة الجزئية في Φ المؤلفة من التحويلات الآتية:

$$G = \{x \mapsto a^{2^{v_2(P^q-1)}}\sigma^{2^{v_2(q)}}(x)+b \ ;\ a\neq 0, b, x\in GF(P^q),\ \sigma \in Aut\ GF(P^q)\}$$

حيث $v_2(p^q-1)$ و $v_2(q)$ أعلى قوة للعامل الأولي 2 في تحليل q و p^q-1 إلى الشكل القانوني على الترتيب عندئذٍ : $A(T)=G$

البرهان:

واضح أن: $\forall g\in G, \forall (x,y)\in U \Rightarrow (x)g),y)g))\in U$

(لأنه إذا كان $(x, y)\in U$ فإن $y-x\in S$ (تعريفاً) وعليه فإن $g(y)-g(x)\in S$ وبالتالي فإن $g(y-x) = g(y)-g(x)\in S$ $((y)g,(x)g))\in U$ وهذا ما يبرهن أن $A(T)\leq G$.

وللبرهان على المساواة يكفي أن نثبت أن $A(T)$ محتواة في الزمرة التآلفية الخطية Φ حيث :

$$\Phi = \{x\mapsto a\sigma(x)+b\ ;\ a\neq 0, b, x\in GF(p^q),\ \sigma\in Aut\ GF(p^q)\ \}$$

ولتحقيق هذا الهدف نبرهن أولاً أن $A(T)$ إبتدائية ولذلك نطبق البند (i) من المبرهنة (1) على الزمرة G فنجد ما يأتي :

$$G \text{ لا إبتدائية } (imprimitive) \Leftrightarrow \exists\ t\in\mathbb{N}^* : \frac{p^q-1}{2^{v_2(p^q-1)+v_2(q)}}\ t = p\ -1 \Longrightarrow$$

$$t=2^{v_2(p^q-1)+v_2(q)} \Longrightarrow \Longrightarrow \frac{p^q-1}{p-1}$$

$$\Longrightarrow \quad (1+ p+.....+p^{q-1})t = 2^m; m \in N^* \Longrightarrow$$

$$\Longrightarrow \quad (1+ p+.....+p^{q-1}) = 2^s \ ; s \in N^* \qquad ①$$

وهذا مستحيل (لأنه إذا كان $q \neq 2$ فإن الطرف الأيسرمن ① عدد صحيح فردي وإذا كان q=2 فإن $1+P= 2^s$ وهذه الحالة مستثناة في نص النظرية)

وهذا ما يبرهن أن الزمرة G إبتدائية وعليه فإن (T)A إبتدائية (لأن $G\leq A(T)$) وسأبرهن أن الزمرة (T)A قابلة للحل .

نلاحظ أنه لا يوجد عنصر φ من (T)A بحيث أن $|\varphi| = 2$ (لأنه لو وجد $|\varphi| = 2$ لوجد ضلع (x,y) بحيث أن $\varphi(x)=y$ و $\varphi(x)=\varphi(y)\varphi^2$ حيث ($\varphi^2= x$) (x) وبما أن φ يحافظ على الأضلاع في U $\in$ U إذن:

$(\varphi(x), \varphi(y)) \in U \Longrightarrow (y, x) \in U$ وهذا مناقض لتعريف T إذن رتبة (T)A لا تقبل القسمة على 2 وعليه فإنه بحسب نظرية *(Feit - Tompson)* [9] تكون (T)A قابلة للحل(لأنها متعدية ورتبتها عدد فردي) وبحسب نتائج [8] يمكن مطابقة مجموعة العقد X للبيان T مع فضاء المتجهات $GF(P^q)$ المعرف على (P)GF بحيث أن:

$$F=(T)A \qquad ② \ A(T)_o$$

$$F=\{x\longmapsto x + b; b\in GF(P^q)\} \qquad \text{حيث}$$

و $A(T)_o$ الزمرة الجزئية المثبتة للصفر في(T)A وهي غير خزولة على $GF(P^q)$.

سأبرهن الآن أن الزمرة $A(T)_o$ إبتدائية .

نميز حالتين :

1) عندما $q|p-1$ نجد أن $p-1=q^\alpha l$ حيث l عدد صحيح و $q\nmid l$ و $\alpha\in\mathbb{N}^*$ ويكون:

$$1+p+p^2+.....+p^{q-1} = 1+(1+q^\alpha l) + (1+q^\alpha l)^2+..... =$$

$$=q(1+a_1 q^{\alpha-1} + a_2 q^{\alpha-2}+..... +a_{q-1}q^{\alpha(q-1)-1})$$

حيث $a_1,.....,a_{q-1}$ أعداد صحيحة متعلقة بالعدد l .

ولنأخذ الزمرة K_0 الجزئية في الزمرة G_0 والمؤلفة من التحويلات التالية :

$$K_0 = \{x \longmapsto a^{2^{v_2(p^q-1)}q^{v_q(p^q-1)}}x \ ; \ a \neq 0, x \in GF\ (p^q)\}$$

فنجد أن $|K_0| = \frac{p^q-1}{2^{v_2(p^q-1)+v_q(p^q-1)}}$.

واضح أن $|K_0|$ يقسم p^q-1 و q لا يقسم $|K_0|$ وبقي أن نبرهن أن $|K_0|$ لا يقسم p –I وبمناقشة مماثلة لما تقدم سنحصل على مساواة مشابهة للمساواة *(1)* :

$$1+a_1 q^{\alpha-1} + a_2 q^{\alpha-2}+.... +a_{q-1}q^{\alpha(q-1)-1}=2^s; s \in \mathbb{N}^* \quad |K_0||p-1 \Leftrightarrow$$

وهذا مستحيل لأن الطرف الأيسرلا يقبل القسمة على 2 (فهو عدد صحيح فردي) وبحسب (iii)

من المبرهنة (1) نجد أن K_0 إبتدائية (لأن $|K_0| \nmid p-1$ & $|K_0| \mid (-1)p^q$ & $q \nmid |K_0|$)
وينتج من ذلك أن $A(T)_o$ إبتدائية (لأن $K_0 \subseteq A(T)_o$)

2) عندما $q \nmid p-1$ نجد أن $q \nmid p^q - 1$ لأن $p^q \equiv p \pmod q$

وعليه فإن $v_q(p^q-1)=0$ وهذا يعني أن هذه حالة خاصة من الحالة السابقة وتكون فيها الزمرة K_0 من الشكل :

$$K_0 = \{x \longmapsto a^{2^{v_2(p^q-1)}} x \quad ; a \neq 0, x \in GF(p^q)\}$$

وهي زمرة إبتدائية (لأنها حالة خاصة من (1)). وبما أن $A(T)_o$ زمرة جزئية من (T)A القابلة للحل (*solvable*) إذن $A(T)_o$ قابلة للحل وإبتدائية .

وينتج من ذلك أن $\overline{G}\, A(T)_o \subseteq$ (لأن $\overline{G}$ هي الزمرة الإبتدائية القابلة للحل العظمى في (LG*(q,p)*

وبالاستفادة من المساواة ② ومن *(ii)* من المبرهنة *(2)* نجد أن:

$$A(T) = FA(T)_o \subseteq F\overline{G} = \{x \longmapsto ax^{p^i} + b \,;\, a \neq 0, b, x \in GF(p^q), \; i = 0,1\ldots, q-1\}$$

وهكذا نكون قد برهنا أن $G \subseteq A(T) \subseteq \Phi$.

بما أن $|A(T)|$ عدد فردي و G أعظم زمرة جزئية في الزمرة Φ من بين مجوعة الزمر ذوات الرتب الفردية (بحسب *(i)* من المبرهنة *(2)*) إذن $A(T) = G$.

النتائج والمناقشة:

برهنت على صحة مبرهنتين ونظرية في حالة الحقل الذي عدد عناصره عدد أولي مرفوع إلى قوة أولية وأوصي بمتابعة البحث عندما تكون القوة غير أولية وأنجزت الخطوات الآتية :

1- الخطوة الأولى: بناء الزمر المتعدية (الإبتدائية واللاإبتدائية (Primitive &Imprimitive)) الجزئية في الزمرة التآلفية الخطية التي تؤثر على حقل منته $GF(p^q)$ حيث p,q عددان أوليان

2-الخطوة الثانية: بناء البيانات التامة الموجهة التي تكون زمرة الأوتومرفيزم لها هي الزمرة الإبتدائية العظمى في الزمرة التآلفية الخطية على $GF(p^q)$.

المراجع:

1. C. H. LI. *On isomorphism of finite Cayley graphs*_a survey, Discrete Math., 246,2002,301-334..

2. DAVE WITTE, EDWARD, D., *Transitive permutation group of prime-square degree*, arxiv:math/ 0012192 vol. 1[Math[GR],2000, 1-28.

3. EDWARD, D.; JOY, M. *Automorphism groups of wreath product digraphs, The Electronic Journal of combinatorics* 16,2009,1-30.

4. PASSMUM, D. *P-solvable double transitive permutation groups*, Pacif. J. of Math. Vol. 26, NO. 3, 1969, 555-577.

5. WIELANDT, H. *Finite permutation groups*, New-York, Academic Press, 1964.

6. MASHHOUR, I.; CHRISTOPH, H. *A number Theoretic Aproach to Sylow r-subgroup of Classical Graphs*, Math. Institute. Univ. of Tuebingen-Germany, 18, N2, 2005, 329-338.

7. BABAY, L.; IMRICH, W. *Tournaments with given regular groups*. Preprint Eotvas Lornad Univ., Budapest, 1976, 329-336.

8. SUPRONENKO, D. A *Genaral Linear Group*, Minsk 1972.

9. FEIT, W.; THOMPSON, J. *Solvability of Group of Odd Order*. Pasibic J. Math 63, 13, No3, 775-1024.