二次多项式的平方取值

沈　光　宇

摘　　要

设F为任意特征不为2的域，$f(x)=\alpha x^2-\beta x+r$是F上二次多项式。令$\overline{F}=F\cup\{\infty\}$，并令$f(\infty)=\alpha$。对任意$a\in\overline{F}$，我们定义了变换$\tau_a$: $\overline{F}\to\overline{F}$. 变换$\tau_a$保持“$f(x)$为平方”这性质不变。利用这组变换，(1)当F为有限域，我们确定了集合$H=\{x\in F \mid f(x)\in F^{*2}\}$及$S=\{f(x)\in F^{*2} \mid x\in F\}$，并计算了它们元素的个数；(2)当F为有理数域，我们讨论了整系数二元二次型$f(x, y)$取平方值问题。考虑方程$f(x, y)=z^2$。如它有一整数解，则必有无限多不等价的解，所有的解都可通过变换τ_a简单地得到；(3)当F为实数域，我们得到一族条件不等式。

1.　设F为任意特征不为2的域，F^*为F中非零元的集合，F^2及F^{*2}分别为F及F^*中平方元的集合。令

$$f(x)=\alpha x^2-\beta x+r \tag{1.1}$$

为F上二次多项式，△是它的判别式，即

$$\triangle=\beta^2-4\alpha r. \tag{1.2}$$

如果$\triangle=0$，那么$f(x)=\alpha\left(x-\frac{\beta}{2\alpha}\right)^2$，我们的问题已无需讨论，因此在下面，如非特别声明，总假设

$$\triangle\neq 0. \tag{1.3}$$

在F中加进符号∞，记$\overline{F}=F\cup\{\infty\}$. 定义

$$F(\infty)=\alpha. \tag{1.4}$$

定义$\overline{F}$上变换τ_a. $a\in\overline{F}$:

如　$a\neq\frac{\beta}{2\alpha},\infty$，$\tau_a=\frac{(\alpha a^2-r)x-(\beta a^2-2ra)}{(2\alpha a-\beta)x-(\alpha a-r)}$，当$x\neq\frac{\alpha a^2-r}{2\alpha-\beta}$，∞，

$$\tau_a\left(\frac{\alpha a^2-r}{2\alpha a-\beta}\right)=\infty;\quad \tau_a(\infty)=\frac{\alpha a^2-r}{2\alpha a-\beta}. \qquad (1.5)_1$$

$$\tau_{\frac{\beta}{2\alpha}}(x)=\tau_\infty(x)=\frac{\beta}{\alpha}-x,\ 当\ x=\neq\infty;\quad \tau_{\frac{\beta}{2\alpha}}(\infty)=\tau_\infty(\infty)=\infty. \qquad (1.5)_2$$

当$a\neq\frac{\beta}{2\alpha}$，∞，$\tau_a$为一分式线性变换，令

$$u=2a^2-r,\quad v=\beta a^2-2ra,\quad w=2\alpha a-\beta, \tag{1.6}$$

可以算得τ_a的行列式为

$$vw-u^2=-f(a)^2. \qquad (1.7)$$

因此τ_a退化当且只当$f(a)=0$，即a为f(x)的根。

我们有

$$f\left(\frac{\beta}{2\alpha}\right)=\frac{-\triangle}{4\alpha}\neq 0,\quad f(\infty)=\alpha\neq 0. \qquad (1.8)$$

设$a\in F$, $f(a)=0$,则$a\neq\frac{\beta}{2\alpha}$. 因为$\alpha a^2=\beta a-r$，因此$\alpha a^2-r=\beta a-2r$另一方面，$r=-\alpha a^2+\beta a$，因此$\alpha a^2-r=2\alpha a^2-\beta a$。由(1.5)$_1$得

$$\text{如}\quad f(a)=0,\ \text{则}\quad \tau_a(x)=a,\ \text{当}\quad x\neq a;\ \tau_a(a)=\infty \qquad (1.9)$$

令$\widetilde{F}=\left\{a\in\overline{F}\ \middle|\ f(a)\in F^*\right\}$。由(1.8)，$\frac{\beta}{2\alpha}$, $\infty\in\widetilde{F}$。

引理 (1·1 设$a,x\in\widetilde{F}$，$y=\tau_a(x)$，则存在$k=k(a,x)\in F^*$使$f(y)=k^2f(x)$。特别我们有$y\in\widetilde{F}$。

证明：(Ⅰ)$a\neq\frac{\beta}{2\alpha}$，$\infty$。仍用记号u，v，w，如(1.6)。

(i)如$x\neq\frac{u}{w}$，∞。$y=\tau_a(x)=\frac{ux-v}{wx-u}$。因此$f(y)=(wx-u)^{-2}g(x)$，这里

$$\begin{aligned}g(x)&=\alpha(ux-v)^2-\beta(ux-v)(wx-u)+r(wx-u)^2\\&=(\alpha u^2-\beta uw+rw^2)x^2-(2\alpha uv+2ruw-\beta vw-\beta u^2)x+(\alpha v^2-\beta vu+ru^2)\\&\equiv g_1x^2-g_2x+g_3.\end{aligned}$$

我们来许算g_1，g_2，g_3。

$$\begin{aligned}g_1&=\alpha u^2-\beta uw+rw^2\\&=\alpha(\alpha^2a^4-2\alpha ra^2+r^2-\beta(2\alpha^2a^3-\alpha\beta a^2-2\alpha ra+\beta r)+r(4\alpha^2a^2-4\alpha\beta a+\beta^2)\\&=\alpha(\alpha^2a^4-2\alpha\beta a^3+(\beta^2+2\alpha r)a^2-2\beta ra+r^2)\\&=\alpha f(a)^2.\\g_2&=2\alpha uv+2ruw-\beta vw-\beta u^2\\&=2((\alpha v+rw)u-\beta vw)-\beta(u^2-vw),\end{aligned}$$

注意到$\alpha v+rw=\alpha(\beta a^2-2ra)+r(2\alpha a-\beta)=\beta(\alpha a^2-r)=\beta u$，利用(1.7)，我们有

$$g_2=\beta(u^2-vw)=\beta f(a)^2$$

同样可算得

$$g_3=rf(a)^2.$$

因此

$$g(x)=f(a)^2f(x).$$

即得 $f(y)=\left(\frac{f(a)}{wx-u}\right)^2f(x)$.

(ii)如$x=\frac{u}{w}$，则$y=\tau_a(x)=\infty$，$f(y)=\alpha$，而$f(x)=w^{-2}(\alpha u^2-\beta uw+w^2)$ $=\alpha w^{-2}f(a)^2$(见(i)中g_1的计算)，因此$f(y)=\left(\frac{w}{f(a)}\right)^2f(x)$。

(iii) 如 $x=\infty$，则 $y=\frac{u}{w}$. 由 (ii) 知 $f(y)=\left(\frac{f(a)}{w}\right)^2 f(x)$.

(II) $a=\frac{\beta}{2\alpha}$，∞. 此时 $y=\tau_a(x)=\frac{\beta}{\alpha}-x$. 容易看出 $f(y)=f(x)$

引理证讫.

定理 1.1，设 $x,y\in\overset{\frown}{F}$. 存在 $a\in\overset{\frown}{F}$ 使 $\tau_a(x)=y$ 的必要充分条件是

$$f(x)f(y)\in F^{*2}. \quad (1.10)$$

证明：必要性可从引理1.1得到. 现在证明充分性.

(I) $x\neq\infty$ $y\neq\infty$ 且 $x+y\neq\frac{\beta}{\alpha}$. 现在有

$$\begin{aligned}f(x)\ f(y)&=\alpha^2x^2y^2-\alpha\beta x^2y-\alpha\beta xy^2+\alpha rx^2+\beta^2xy+\alpha ry^2-\beta rx-\beta ry+r\\&=(r-\alpha xy)^2-(\alpha(x+y)-\beta)(\beta xy-r(x+y))\in F^{*2}\end{aligned}$$

考虑a的二次方程式

$$(\alpha(x+y)-\beta)a^2+2(r-\alpha xy)a+(\beta xy-r(x+y))=0. \quad (1.11)$$

它的判别式恰为 $4f(x)f(y)\in F^{*2}$，因此 (1.11) 有解. 首先，此解 $a\neq\frac{\beta}{2\alpha}$. 事实上，(1.11) 可改写为

$$((2\alpha a-\beta)x-(\alpha a^2-r))y=(\alpha a^2-r)x-(\beta a^2-2ra). \quad (1.12)$$

如 $a=\frac{\beta}{2\alpha}$，代入 (1.12)，由于 $\alpha a^2-r=\frac{\triangle}{4\alpha}$，$\beta a^2-2ra=\frac{\triangle}{4\alpha}\cdot\frac{\beta}{\alpha}$，我们将得到 $\triangle(x+y-\frac{\beta}{\alpha})=0$. 由(1.3)，$x+y-\frac{\beta}{\alpha}=0$，与假设不符.

另外，$f(a)\neq 0$. 事实上，如 $f(a)=0$，从 (1.9) 的计算知 $\alpha a^2-r=\beta a-2r=2\alpha a^2-\beta a$，因此 (1.12) 成为 $y=a$，与假设 $y\in\overset{\frown}{F}$ 矛盾.

由此，$x\neq\frac{\alpha a^2-r}{2\alpha a-\beta}$。因为否则 (1.12) 左端为 0，右端也应为 0，即得，$\frac{\beta a^2-2ra}{\alpha a^2-r}=x=\frac{\alpha a^2-r}{2\alpha a-\beta}$. 从 (1.1) 得 $f(a)=0$，不可能.

这样，从 (1.12) 即得 $y=\tau_a(x)$.

(II) $x\neq\infty$，$y\neq\infty$ 而 $x+y=\frac{\beta}{\alpha}$. 令 $a=\frac{\beta}{2\alpha}$，则 $y=\tau_a(x)$ 而 $a\in\overset{\frown}{F}$ (见(1.8)).

(III) $x=\infty$，$y\neq\infty$. $f(x)f(y)=\alpha f(y)=\alpha^2y^2-\alpha(\beta y-r)\in F^{*2}$. 考虑二次方程

$$\alpha a^2-2\alpha ya+(\beta y-r)=0. \quad (1.13)$$

它的判别式为 $4f(x)f(y)\in F^{*2}$，所以有解. 此解 $a\neq\frac{\beta}{2\alpha}$，否则代入 (1.3) 得 $\frac{\triangle}{4\alpha}=0$，与 (13) 矛盾. 此外，$f(a)\neq 0$，否则由 (1.13)，$y=\frac{\alpha a^2-r}{2\alpha a-\beta}=\frac{(2\alpha a^2-\beta)a-f(a)}{2\alpha a-\beta}=a$，如 $f(a)=0$ 这与 $y\in\overset{\frown}{F}$ 矛盾. 由 $(1.5)_1$，$y=\tau_a(x)$.

(IV) $x\neq\infty$，$y=\infty$，和(III)同样可证.

(V) $x=\infty$，$y=\infty$. 令 $a=\infty\in\overset{\frown}{F}$，$y=\tau_\infty(x)$. 定理证讫

对任意$a\in\overline{F}$，我们定义

$$a^*=\frac{\beta a-2r}{2\alpha a-\beta}，当\ a\neq\frac{\beta}{2\alpha}，\infty；\ \left(\frac{\beta}{2\alpha}\right)^*=\infty；\ \infty^*=\frac{\beta}{2\alpha}.$$

当$a\neq\frac{\beta}{2\alpha}$，$\infty$，（1.14）可写为

$$2\alpha a a^*-\beta(a+a^*)+2r=0. \tag{1.15}$$

此式对a，a^*是对称的，因此有

$$a^{**}=a. \tag{2.16}$$

如果$a=a^*$，由（1.15）得$2f(a)=0$．反之，$f(x)=0$则$a=a^*$．

$$a^*\neq a，当 a\in\overline{F}, \tag{1.17}$$

$$若\ a\ \overline{\in} F，则 a^*\in\overline{F}. \tag{1.18}$$

定理1.2　设a，b，$t\in\overline{F}$，$a\neq b$．则$\tau_a(t)=\tau_b(t)$的必要充分条件是$b=a^*$．

证明：必要性：(Ⅰ)$t\neq\infty$．(i)若$a=\frac{\beta}{2\alpha}$．$\tau_b(t)=\tau_{\frac{\beta}{2\alpha}}(t)=\frac{\beta}{\alpha}-t$．若$b\neq\infty$，这时$t\neq\frac{\alpha b^2-r}{2\alpha b-\beta}$，否则$\tau_b(t)=\infty$，不可能．我们应有

$$\frac{(\alpha b^2-r)t-(\beta b^2-2rb)}{2(\alpha b-\beta)t-(\alpha b^2-r)}=\tau_b(t)=\frac{\beta}{\alpha}-t,$$

即

$$((\alpha b^2-r)t-(\beta b^2-2rb)\left(\frac{\beta}{\alpha}-t\right)=(2\alpha b-\beta)t-(\alpha b^2-r).$$

即

$$(2\alpha b-\beta)(\alpha t^2-\beta t+r)=0.$$

$b\neq a=\frac{\beta}{2\alpha}$，因此有$f(t)=0$，与$t\in\overline{F}$的假设矛盾．因此必须有$b=\infty$．

(ii)如$a=\infty$，和(i)完全一样可证$b=\frac{\beta}{2\alpha}$．

(iii)$a\neq\frac{\beta}{2\alpha}$，$\infty$；$t=\frac{\alpha a^2-r}{2\alpha a-\beta}$．由(i)（交换$a$，$b$位置），可知$b\neq\frac{\beta}{2\alpha}$或$\infty$．$\tau_b(t)=\tau_a(t)=\infty$，因此$t=\frac{\alpha b^2-r}{2\alpha b-\beta}$．故有$\frac{\alpha b^2-r}{2\alpha b-\beta}=\frac{\alpha a^2-r}{2\alpha a-\beta}$．

即

$$(\alpha b^2-r)(2\alpha a-\beta)=(\alpha a^2-r)(2\alpha b-\beta). \tag{1.19}$$

由此可得$\alpha(a-b)(2\alpha ab-\beta(a+b)+2r)=0$．由（1.15）．即$b=a^*$

(iv)$a\neq\frac{\beta}{2\alpha}$，$\infty$，$t\neq\frac{\alpha a^2-r}{2\alpha a-\beta}$．和上面一样可知$b\neq\frac{\beta}{2\alpha}$，$\infty$，且$t\neq\frac{\alpha b^2-r}{2\alpha b-\beta}$．由（1.5）$_1$，$\tau_a(t)=\tau_b(t)$即

$$\begin{aligned}&((\alpha a^2-r)t-(\beta a^2-2ra))((2\alpha b-\beta)t-(\alpha b^2-r))\\&=((\alpha b^2-r)t-(\beta b^2-2rb))((2\alpha a-\beta)t-(\alpha a^2-r))\end{aligned} \tag{1.20}$$

展开，简化，得$\alpha(a-b)f(t)(2\alpha ab-\beta(a+b)+2r)=0$．因$a\neq b$，$f(t)\neq0$，我们就得到$b=a^*$

(II) $t=\infty$。很明显，若 $a=\frac{\beta}{2\alpha}$ 或 ∞，则 $\tau_a(t)=\tau_b(t)=\infty$。因此必须有 $b=\infty$ 或 $\frac{\beta}{2\alpha}$ 即 $b=a^*$。

若 $a\neq\frac{\beta}{2\alpha},\infty$，则 $b\neq\infty$，$\frac{\beta}{2\alpha}$，$\tau_a(\infty)=\tau_a(\infty)$ 即 $\frac{\alpha a^2-r}{2\alpha a-\beta}=\frac{\alpha b^2-r}{2\alpha b-\beta}$。和(I)(iii)一样有 $b=a^*$。

充分性：(I) $t\neq\infty$。(i) $a=\frac{\beta}{2\alpha}$ 或 ∞，则 $b=a^*=\infty$ 或 $\frac{\beta}{2\alpha}$。由 $(1.5)_2$ 即有 $\tau_a(t)=\tau_b(t)$。

(ii) $a\neq\frac{\beta}{2\alpha}$，$\infty$ 而 $t=\frac{\alpha a^2-r}{2\alpha a-\beta}$。从条件 $b=a^*$ 可逆推得(1.19)(参看必要性(I)(iii)的证明)。我们指出：$2\alpha b-\beta\neq0$。事实上，若 $2\alpha b-\beta=0$，由(1.19)，必须有 $\alpha b^2-r=0$。以 $b=\frac{\beta}{2\alpha}$ 代入得 $\frac{\triangle}{4\alpha}=0$，与(1.3)矛盾。因此，从(1.19)即得 $t=\frac{\alpha a^2-r}{2\alpha a-\beta}=\frac{\alpha b^2-r}{2\alpha b-\beta}$ 从 $(1.5)_1$ 即知 $\tau_a(t)=\tau_b(t)=\infty$。

(iii) $a\neq\frac{\beta}{2\alpha}$，$\infty$，而 $t\neq\frac{\alpha a^2-r}{2\alpha a-\beta}$。从(ii)可知 $t\neq\frac{\alpha b^2-r}{2\alpha b-\beta}$。从条件 $b=a^*$ 可逆推得(1.20)，从此即可知 $\tau_b(t)=\tau_a(t)$。

(II) $t=\infty$。若 $a=\frac{\beta}{2\alpha}$ 或 ∞，则 $b=\infty$。或 $\frac{\beta}{2\alpha}$，所以 $\tau_a(t)=\tau_b(t)$。如 $a\neq\frac{\beta}{2\alpha}$，$\infty$，从 $b=a^*$ 可逆推得 $\frac{\alpha a^2-r}{2\alpha a-\beta}=\frac{\alpha b^2-r}{2\alpha b-\beta}$(见必要性证明(I)(iii))，因此 $\tau_a(\infty)=\tau_b(\infty)$。引理证讫。

系1.1 设 $c\in\widetilde{F}$，$Hc=\left\{x\in\widetilde{F}\;\middle|\;f(x)\in f(c)F^{*2},\right\}$ 则 $Hc=\left\{\tau_a(c)\mid a\in\widetilde{F}\right\}$。

特别有

系1.2 设 $c\in\widetilde{F}$，$f(c)\in F^{*2}$。令 $\overline{H}=\left\{x\in\overline{F}\mid f(x)\in F^{*2},\right\}$。

则 $\overline{H}=\left\{\tau_a(c)\mid a\in\widetilde{F}\right\}$。

2．在本节中，假定F为有限域(特征不为2)。如S为任一有限集，我们将用符号 $|S|$ 表S中元素的个数。设

$$|F|=q. \tag{2.1}$$

则

$$|\widetilde{F}|=q+1 \tag{2.2}$$

$\widetilde{F}=\overline{F}$ 当 $\triangle\notin F^{*2}$，$\widetilde{F}=\overline{F}\mid\left\{x_1,x_2\right\}$，当 $\triangle\in F^{*2}$，这里 x_1，x_2 是 $f(x)$ 的二根。因此

$$|\widetilde{F}|=q+1，当\triangle\notin F^{*2}; \tag{2.3$_1$}$$

$$|\widetilde{F}|=q-1，当\triangle\in F^{*2}. \tag{2.3$_2$}$$

引理 2.1 设 $K=\left\{f(a)\mid a\in F\right\}$。对 $k\in K$，令 $T_k=\left\{t\in F\mid f(t)=k\right\}$。令

$$k_0 = -\frac{\triangle}{4\alpha}. \tag{2.4}$$

则 $|T_k| = 1$，当 $k = k_0$； $|T_k| = 2$，当 $k \neq k_0$。

证明： $f(t) = k$ 即 $\alpha t^2 - \beta t + (r - K) = 0$． $|T_k| = 1$，即此方程有重根，也即它的判别式 $\beta^2 - 4\alpha(r-k) = 0$，由此即得 $k = k_0$。

系 2.1 令 $K = \left\{ f(t) \mid t \in F \right\}$，则 $|K| = \frac{1}{2}(q+1)$。

证明：$F = \bigcup_{K \in K} T_k$，因此 $|F| = 2(|K| - 1) + 1$，即 $K = \frac{1}{2}(|F| + 1)$。

定理 2.1 设 $H = \left\{ x \in F \mid f(x) \in F^{*2} \right\}$，$h = |H|$．则（Ⅰ）若 $\triangle = 0$，$h = q - 1$，当 $\alpha \in F^{*2}$；$h = 0$，当 $\alpha \overline{\in} F^{*2}$。（Ⅱ）若 $\triangle \in F^{*2}$，则 $h = \frac{1}{2}(q-3)$，当 $\alpha \in F^{*2}$；$h = \frac{1}{2}(q-1)$，当 $\alpha \overline{\in} F^{*2}$。（Ⅲ）若 $0 \neq \triangle \overline{\in} F^{*2}$，则 $h = \frac{1}{2}(q-1)$，当 $\alpha \in F^{*2}$；$h = \frac{1}{2}(q+1)$，当 $\alpha \overline{\in} F^{*2}$。

证明：若 $\triangle = 0$，则 $f(x) = \alpha(x - x_0)^2$，结论是显然的．设 $\triangle \neq 0$．令 $\overline{H} = \left\{ x \in \overline{F} \,\middle|\, f(x) \in F^{*2} \right\}$．任取 c 使 $f(c) \neq 0$．定义 Hc 如系1．1．由定理1．2，对 Hc 中任一元 t，恰有二个 $a \in \widetilde{F}$ 使 $\tau_a(c) = t$．因此 $|Hc| = \frac{1}{2}|\widetilde{F}|$．(1)如 $\alpha \in F^{*2}$，则 $\overline{H} = Hc$；(2)如 $c \overline{\in} F^{*2}$，$\overline{H} = \widetilde{F}/Hc$．在二种情况下，我们都有 $|\overline{H}| = \frac{1}{2}|\widetilde{F}|$．当 $\alpha \in F^{*2}$，$\infty \in \overline{H}$，此时 $H = \overline{H}/\{\infty\}$，因此 $|H| = \frac{1}{2}|\widetilde{F}| - 1$；当 $\alpha \overline{\in} F^{*2}$，$\infty \overline{\in} \overline{H}$，此时 $H = \overline{H}$，因此 $|H| = \frac{1}{2}|\widetilde{F}|$．以（2．3）代入即得（Ⅱ）及（Ⅲ）.

系2．2 设 $f(x)$ 为有限域 F（特征不为2）上的二次多项式．所有 $f(x)$ 的非0值都为平方（都为非平方）当且只当 $f(x) = \alpha(x - x_0)^2$，其中 α 为平方（非平方）。

系2．3 令 $G = \left\{ \frac{\alpha a^2 - r}{2\alpha a - \beta} \,\middle|\, a \in F,\ a \neq \frac{\beta}{2\alpha} \right\}$，$H$ 定义如定理2.1.则 $H = G$ 当 $\alpha \in F^{*2}$；$H = F/G$ 当 $\alpha \overline{\in} F^{*2}$。

证明：$G = \left\{ \tau_a(\infty) \,\middle|\, a \in F,\ a \neq \frac{\beta}{2\alpha} \right\}$．由系1．1．（1．4），（1.5）即可得到结论。

定理2．2 设 $S = \left\{ K \in F^{*2} \mid f(x) = K,\ x \in F \right\}$，$s = |S|$，则 (I) 若 $\triangle = 0$，$s = \frac{1}{2}(q-1)$ 当 $\alpha \in F^{*2}$；$s = 0$，当 $\alpha \overline{\in} F^{*2}$．(II)若 $0 \neq \triangle \in F^{*2}$，(i) $s = \frac{1}{4}(q-1)$ 当 $\alpha \in F^{*2}$，$-1 \in F^{*2}$；(ii) $s = \frac{1}{4}(q-3)$，当 $\alpha \in F^{*2}$，$-1 \overline{\in} F^{*2}$；(iii) $s = \frac{1}{4}(q-1)$，当 $\alpha \overline{\in} F^{*2}$，$-1 \in F^{*2}$；(iv) $s = \frac{1}{4}(q+1)$，当 $\alpha \overline{\in} F^{*2}$，$-1 \overline{\in} F^{*2}$；(III)若 $0 \neq \triangle \overline{\in} F^{*2}$，(i) $s = \frac{1}{4}(q-1)$,

当$\alpha\in F^{*2}$，$-1\in F^{*2}$；(ii)$S=\frac{1}{4}(q+1)$，当$\alpha\in F^{*2}$，$-1\bar{\in}F^{*2}$；(iii)$S=\frac{1}{4}(q+3)$，当$\alpha\bar{\in}F^{*2}$，$-1\in F^{*2}$；(iv)$s=\frac{1}{4}(q+1)$，当$\alpha\bar{\in}F^{*2}$，$-1\bar{\in}F^{*2}$。

证明：(I)是显然的．若$\triangle\neq 0$，由引理2．1，如$k_0=-\frac{\triangle}{4\alpha}\bar{\in}F^{*2}$，则H中每二元素对应于S中一元素，因此，$s=\frac{1}{2}h$．反之，如$K_0\in F^{*2}$，则$s=\frac{1}{2}(h-1)+1=\frac{1}{2}(h+1)$．因此，(II)$\triangle\in F^{*2}$,(i)$\alpha\in F^{*2}$,$-1\in F^{*2}$,此时$K_0\in F^{*2}$而$h=\frac{1}{2}(q-3)$（见定理2．1），因此$s=\frac{1}{2}(h+1)=\frac{1}{4}(q-1)$．(ii)——(iv)可同样证明．（III）$\triangle\bar{\in}F^{*2}$，(i)$\alpha\in F^{*2}$，$-1\in F^{*2}$此时$K_0\bar{\in}F^{*2}$，而$h=\frac{1}{2}(q-1)$，因此 $S=\frac{1}{2}h=\frac{1}{4}(q-1)$．(ii)——(iv)可同样算得．

注　$-1\in F^{*2}$当且只当$q=4n+1$，$-1\bar{\in}F^{*2}$当且只当$q=4n-1$，因此定理2．2中S都是整数．

系2．4　令 $T=\left\{\alpha\left(\frac{(f(a)}{2\alpha a-\beta}\right)^2\,\middle|\, a\in F,\ a\neq\frac{\beta}{2\alpha}\right\}$．则$S=T$，当$\alpha\in F^{*2}$；$S=K^*/T$，当$\alpha\bar{\in}F^{*2}$，这里$K^*=\left\{f(a)\,\middle|\, a\in F,\ f(a)\neq 0\right\}$．

证明：从引理1．1中g_1的计算可知$T=\left\{f(x)\,\middle|\, X\in G\right\}$（G的定义见系2．3）．而$G==H=\left\{x\in F\,\middle|\, f(x)\in F^{*2}\right\}=\left\{x\in F\,\middle|\, f(x)\in S\right\}$当$\alpha\bar{\in}F^{*2}$，因此$S=\left\{f(x)\,\middle|\, x\in G\right\}=T$．如$\alpha\bar{\in}F^{*2}$，$G=\left\{x\in F\,\middle|\, f(x)\in K^*/S\right\}$，因此$S=K^*/T$．

3．设R为有理数域，I为整数环．仿照§1中关于F的定义我们定义I^*，I^2，I^{*2}等，考虑整系数二次型

$$P(x,\ y)=\alpha x^2-\beta xy+\gamma y^2,\ \alpha,\ \beta,\ \gamma\in I, \tag{3.1}$$

其中

$$\alpha\neq 0. \tag{3.2}$$

我们仍设（1．3）成立．

我们称I上2维非0向量$(x,\ y,\ )$和$(x',\ y')$为等价，如果存在$k\in R$，$k\neq 0$，使$(x,\ y)=k(x',\ y')$，记为$(x,y)\sim(x',y')$．很明显，如$(x,y)\sim(x',y')$，则$P(x,\ y)=k^2P(x',\ y')\in I$，因此

$$P(x,\ y)\in I^{*2}\quad 当且只当\quad P(x',\ y')\in I^{*2}. \tag{3.3}$$

以$(x,\ y)^*$表$(x,\ y)$所属的等价类．作对应$(x,\ y)^*\to x/y$，当$y\neq 0$；$(x,\ 0)^*\to\infty$.这是$\left\{(x,y)^*\right\}$到$\bar{R}=R\cup\left\{\infty\right\}$上的一一对应．下面我们将等同$(x,\ y)^*$和$x/y$（或$\infty$）而不加区分．

定理3．1　设$A=\left\{(x,\ y)\,\middle|\, P(x,\ y)\in I^{*2}\right\}$，$(x_0,\ y_0)\in A$．则A中有无限个

互不等价的元素且$A=\bigcup\limits_{a\in\widetilde{R}}\tau_a((x_0, y_0)^*)$。

证明：设(x, y)为I上2维非0向量. 如$y\neq 0$,则$p(x,y)=y^2f\left(\frac{x}{y}\right)$,这时$p(x,y)\in I^{*2}$当且只当$f((xy)^*)=f\left(\frac{x}{y}\right)\in R^{*2}$。如$y=0$, $p(x, 0)=\alpha x^2$,同样也有$p(x, 0)\in I^{*2}$当且只当$f((x, 0)^*)=f(\infty)=\alpha\in R^{*2}$。

设$(x_0, y_0)\in A$, 则$f((x_0, y_0)^*)\in R^{*2}$。由定理1. 1, $f((x, y)^*)\in R^{*2}$当且只当$(x, y)^*=\tau_a((x_0y_0)^*)$, 对某$a\in\widetilde{R}$. 这就证明了$A=\bigcup\limits_{a\in\widetilde{R}}\tau_a((x_0, y_0)^*)$A有无限个不等价元素可由定理1. 2立即得到.

注　假设(3. 2)并不妨碍定理3. 1的普遍性. 事实上，如$\alpha=0$而$r\neq 0$，则交换x，y的位置就可以了. 如$\alpha=r=0$. 此时$P(x, y)=-\beta xy$. 令$y=x+z$，代入得$P'(x, z)=P(x, y)=-\beta x^2-\beta xz$即满足(3. 2)。

例　如α或r属于I^{*2}，则A非空，因为(1, 0)或(0, 1)属于A. 又，如$-\frac{\triangle}{4\alpha}\in R^{*2}$则$f\left(\frac{\beta}{2\alpha}\right)\in R^{*2}$,因此$(\beta, 2\alpha)\in A$. 在这些情形，$P(x, y)\in I^{*2}$的所有解可用定理3. 1求出。特别，令$P(x, y)=x^2+y^2$. 用$(1. 5)_1$，$(1. 5)_2$. 当$a\neq 0, 1$, $\tau_a(0)=\frac{2a}{1-a^2}$，设$a=\frac{m}{n}$，$m\neq n$，则$\tau_a(0)=\frac{2mn}{n^2-m^2}$，$\tau_1(0)=\infty=(1, 0)^*$，因此$A=\bigcup\limits_{m,n\neq 0\ (m\neq n)}(2mn, n^2-m^2)\cup(1, 0)^*\cup(0, 1)^*$. 因此$(x, y)$为$x^2+y^2=z^2$的整数解，$x\neq 0$，$y\neq 0$，当且只当$(x, y)\sim(2mn, n^2-m^2)$，$m,n\neq 0$，$m\neq n$这是熟知的结果.

上面的方法也适用于任何交换整环及其商域.

4. 设F为实数域. 问题成为解二次不等式.

定理4. 1　设$f(x)$为实系数二次多项式，首项系数$\alpha>0$，如$f(x)$有二根$x_1, x_2, x_1<x_2$则$x_1<x<x_2$的必要充分条件是$x_1<\tau_a(x)<x_2$，对任$-a\in\widetilde{F}$.

证明：我们知道$f(x)<0$的必要充分条件是$x_1<x<x_2$，另一方面，由系1. 1，若$f(x)<0$，则$f(x')<0$的必要充分条件是$x'=\tau_a(x)$对任$-a\in\widetilde{F}$. 由此即可得到我们的结论.

例.　$f(x)=x^2-r^2$，则$\tau_a(x)=\frac{(a^2+r^2)x-2r^2a}{2ax-(a^2+1)}$ $(a\neq\pm r)$. 所以当

$$|x|<r. \tag{4. 1}$$

时有

$$\left|\frac{(a^2+r^2)x-2r^2a}{2ax-(a^2+r^2)}\right|<r, \tag{4. 2}$$

对所有$a\neq\pm r$. 反之，如(4. 2)对某一$a\neq\pm r$成立，则必有(4. 1).

注. 如$f(x)$首项系数$\alpha<0$，则只要考虑$-f(x)$就可以了.

［注］ 变换τ_a有下列简单的几何解释。令P为＝维向量空间，$\overline{P}$为P中所有直线的集合。设$O \neq \chi \in P$，我们以$\hat{x}$表χ所属的直线。在P上空义内积$f(x \cdot y) = \alpha x_1 y_1 - \frac{\beta}{2}((x_1 y_2 + x_2 y_1) + \alpha x_2 y_2$，这里$x = (x_1, x_2)$，$y = (y_1 y_2)$。设$D(\overline{D})$为P中非迷向向量(非迷向直线)的集合。对$a \in D$，考虑关于垂直于a的直线的反射

$Ta: Ta(x) = x - \frac{2f(\chi, a)}{f(a,a)}a$。Ta实际上只与$\hat{a}$有关，所以也可记为$T\hat{a}$、对任意$O \neq x = (x_1, x_2) \in P$，$\hat{x}$可用纯量$x_1/x_2$表示（当$x_2 = O$，则记为$\infty$）。因此$\overline{P}$可等同于集合$\overline{F}$。考虑$T\hat{a}$在$\overline{P}$上诱导的变换$\overline{T}\hat{a}$。上面的表示方法下，$\overline{T}\hat{a}$正好成为（1·5）所定义的$\tau_a$，这里$a \in \overleftrightarrow{F}$。$\overline{D}$中每一直线的向量，其长度皆属于$F^*/F^{*2}$的同一傍系u中，这样的直线的集合我们记为$\overline{D}_u$显然$\overline{D}_u$在$\overline{T}\hat{a}$下不变。定理1．1说明$\overline{D}_u$是变换集合$\{T_{\hat{a}}$下的可递区，而定理1．2说明若$\hat{a}$，$\hat{b} \in \overline{D}$且$\hat{a} \perp \hat{b}$，则$\overline{T}\hat{a} = \overline{T}\hat{b}$。

利用上面的几何想法，我们可以把本文中所有结果推广到多元二次多项式的情形。

参 考 文 献

1, Jacobson, N, Lectures in Abstract Algebra, voI.I, van Nostrand, 1951.

2. ——, Lectures in Abstract Algebra, vol. II, van Nostrand, 1964.

The square Values of a Quadratic Polynormial

Shen Guang－Yu

Abstract

Lef f(x) be a quadratic polynomial with cocfficients in a finite field F、On how many points of F can f(x) take values which are squares in F? How. many square values can f(x) take? How do we determine these points and values? We solve these problems by applying a set of transformations of F into itself which preserve the property "f(x) is a square".

The transformations can be defined on an arbitrary field as well. When F is the field of rational numbers they can be used to discuss the square values of a quadratic form of two variadles f(x.y) with integral coefficients. If there exists one point (x_0, y_0), where x_0 and y_0 are integers, such that $f(x_0, y_0)$ is a square of an integer then there are infinitely many others, all of them can easily be obtained by means of the transformations. A family ofconditional inequalities is obtaiued when they are applied of reals.