Ist nämlich $A \in \Sigma$ – falls $\ell \equiv 3 \bmod 4$, bzw. $A \in \Phi - \Sigma$ – falls $\ell \equiv 1 \bmod 4$, so enthält A ein Primideal $\mathfrak{p}$ ersten Grades; für dieses Primideal gilt dann $\left(\frac{N(\mathfrak{p})}{\ell}\right) = +1$ – für $\ell \equiv 3 \bmod 4$ – bzw. $\left(\frac{N(\mathfrak{p})}{\ell}\right) = -1$ für $\ell \equiv 1 \bmod 4$, in jedem Fall $N(\mathfrak{p}) \not\equiv 0, -1 \bmod \ell$, daher – da $N(\mathfrak{p})$ eine Primzahl ist – $N(\mathfrak{p}) \in R^*$.

Da d mindestens einen von ℓ verschiedenen Primfaktor enthält, gibt es nach bekannten Schlüssen eine Primzahl p mit

$$\left(\frac{d}{p}\right) = +1, \quad \left(\frac{p}{\ell}\right) = -1, \quad p \not\equiv 0, -1 \bmod \ell$$

(hier wird zum ersten Mal benutzt, daß $\ell \geqq 5$ ist!); ist daher $p = N(\mathfrak{p})$ für ein geeignetes Primideal $\mathfrak{p}$, A die zu $\mathfrak{p}$ gehörende (verallgemeinerte) Idealklasse, so ist

$$A \in (\Phi - \Sigma) \cap \Gamma.$$

Fassen wir zusammen, so haben wir

$$[\Phi : \Sigma] = 2$$

und

$$\Sigma \subsetneqq \Gamma \quad \text{für } \ell \equiv 3 \bmod 4,$$

$$\emptyset \neq \Phi - \Sigma \subseteq \Gamma \quad \text{für } \ell \equiv 1 \bmod 4,$$

in jedem Fall also $\Gamma = \Phi$. $\square$

<u>Lemma 2</u>

<u>Es gibt ein</u> $T \in GL_r(R)$, <u>sodaß</u>

$$Q(Tx) = \alpha_1 x_1^2 + \alpha_2 x_2^2 + \dots + \alpha_r x_r^2$$

<u>für geeignete Zahlen</u> $\alpha_1, \alpha_2, \dots, \alpha_r \in R$.