Eventuell führt dies nicht zum Ziel, da die Koeffizienten l in $T(l)$ zu groß werden, deshalb

while (rg $B < d$ & # Zeile $B > d$)

bei ⊛, und falls man mit rg $B < d$ abbricht, erhöhe t_{ep} und nochmal.

In der Tat benötigt man $t_{ep} \sim 1000$ da man jetzt je 100 F tabellieren kann.

Annahme: haben $f_1, \ldots, f_d$ Basis von $S_k^{new}(m)$ (etwa Koeff. in $\mathbb{Q}$)

<u>Berechnung der p_j, F_j:</u>

$$B = \left(\ldots, \begin{matrix} \text{Spalte der} \\ \text{erste } t_{ep} \\ \text{Koeff. von } f_j \end{matrix}, \ldots \right) \in \mathbb{Q}^{t_{ep} \times d}, \quad p \text{ erste Primzahl mit } p \nmid m.$$

do {

berechne $M(p) \in \mathbb{Q}^{d \times d}$ mit $T(p)(f_1, \ldots, f_d) = (f_1, \ldots, f_d) M(p)$;

zerlege $\det(M(p) - X \cdot \mathbb{1}) = \underbrace{X_1 \cdots X_r}_{=: \ldots} \psi_1^{g_1} \cdots \psi_s^{g_s}$

$(X_j, \psi_j \in \mathbb{Z}[X]$ irred., $g_j > 1)$;

for $j \in 1, \ldots, r$:

{ berechne Spalte $v_j \in \underbrace{\mathbb{Q}[X]/X_j}_{=: k_j}$ mit $(M(p) - X) v_j \equiv 0$ (in k_j);

$F_j := B \cdot v_j$;

}

$B = B \cdot \mathrm{Kern}\, X(M(p))$;

$p =$ nächste Primzahl $> p$ mit $p \nmid m$;

} while $(s > 0)$

vgl. 5a

<u>Bemerkungen:</u> 1) $p \nmid m$, weil (falls $p \mid m$, so: Eigenwerte von $T(p) = \pm p^{k/2}$, also $\mathrm{char}\, T(p) = (X + p^{k/2})^{\alpha} (X - p^{k/2})^{\beta}$.

2) nicht wirklich Algorithmus, kann sein daß $\mathrm{char}\, T(p)$ <u>nie</u> quadratfrei!

Fall $N = 512$, in der Praxis haben berechnet

k	2	4	6	8	10	12
t_{ep}	1000	200	100	60	40	30

4 Formen, alle zueinander konjugiert

$\mathrm{Char}(T(p), R) = \psi_p^2$ (je zwei haben jeweils gleiche EW, oder verschiedene zwei)

tritt bei Nebentyp ständig auf