G. Nebe, M. Kirschmer

Lösung 9

Aufgabe 1.
Sei $b_n = a_n - a_{n-1} = -f(a_{n-1})/f'(a_{n-1})$. Aus der Vorlesung wissen wir:

- $v(f(a_n)) \geq 2v(b_n) > v(f(a_{n-1}))$ für alle $n \in \mathbb{N}$.
- $v(f'(a_n)) = v(f'(a_{n-1}))$ für alle $n \in \mathbb{N}$.

Jetzt zu den Abschätzungen.

(a) Wir führen Induktion nach n. Im Fall $n = 0$ ist $v(f(a_0)) > 2v(f'(a_0)) \geq v(f'(a_0))$ wie behauptet. Für $n \geq 1$ wird

$$\begin{aligned} v(f(a_n)) &\geq 2v(b_n) = 2v(f(a_{n-1})) - 2v(f'(a_{n-1})) \\ &\geq 2(2^{n-1} - 1)d - 2v(f'(a_0)) \\ &= (2^n - 1)d - (d + 2v(f'(a_0))) \\ &= (2^n - 1)d - v(f(a_0)) \,. \end{aligned}$$

(b) Für alle $n \geq 1$ ist

$$\begin{aligned} v(a_n - a_{n+1}) &= v(b_{n-1}) = v(f(a_n)) - v(f'(a_n)) \\ &> v(f(a_{n-1})) - v(f'(a_{n-1})) \\ &= v(b_{n-1}) = v(a_{n-1} - a_n) \,. \end{aligned}$$

Also ist die Folge $(v(a_n - a_{n+1}))_n$ monoton wachsend.
Für jedes $k > n$ ist dann

$$v(a_n - a_k) = v(\sum_{i=n}^{k-1}(a_i - a_{i+1})) = v(a_n - a_{n+1}) = v(b_{n+1}) = v(f(a_n)) - v(f'(a_n)) \,.$$

Insbesondere ist damit auch $v(a_n - a) = v(f(a_n)) - v(f'(a_n))$.

(c) Folgt aus (a) und (b), denn es ist

$$v(a_n - a) = v(f(a_n)) - v(f'(a_0)) \geq (2^n - 1)d + \underbrace{v(f(a_0))}_{\geq d} - v(f'(a_0)) \geq 2^n d - v(f'(a_0)) \,.$$

Aufgabe 2.

(a) Wir betrachten $f(X)$ mod 3. Es wird $f(0) = -1$, $f(1) = 1$ und $f(-1) = -1$. Also existieren keine Nullstellen modulo 3 und somit keine in $\mathbb{Z}_3$.

(b) Wir betrachten $f(X)$ mod 5. Es ist $f(3) = (3)^3 - 2 = 25$ und $f'(3) = 3(3)^2 = 27$. Also liftet die Nullstelle $a_0 = 3 \in \mathbb{F}_5$ zu einer Nullstelle $a \in \mathbb{Z}_5$. Es ist $d := v_5(f(a_0)) - 2v_5(f'(a_0)) = 2$. Nach Aufgabe 1c gilt damit $v_2(a_n - a) \geq 2^n \cdot 2$. Also müssen wir $n = 2$ wählen um eine Näherung 6. Ordnung zu erhalten:

Es wird $a_1 = 3 - \frac{25}{27} = \frac{56}{27}$ und $a_2 = \frac{56}{27} - \frac{f(a_1)}{f'(a_1)} = \frac{56}{27} - \frac{136250}{19683}\frac{243}{3136} = \frac{195299}{127008}$. Der Standardvertreter von $a_2 + 5^6\mathbb{Z}_5$ in $\{0, 1, \ldots, 5^6 - 1\}$ ist 5303.

Also liefert $5303 = 3 + 0 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 3 \cdot 5^4 + 1 \cdot 5^5$ die ersten sechs Stellen von a in der Standarddarstellung.

Angenommen es existieren noch weitere Nullstellen von f in $\mathbb{Z}_5$, so würde f über $\mathbb{Z}_5$ und somit über $\mathbb{F}_5$ in Linearfaktoren zerfallen. Über $\mathbb{F}_5$ ist aber $f(X) = (X + 2)(X^2 - 2X - 1)$ und der zweite Faktor ist bereits irreduzibel wie man durch Einsetzen aller Elemente aus $\mathbb{F}_5$ feststellt.

(c) Wir betrachten $f(X)$ mod 3. Es wird $f(0) = 0$ und $f(-1) = f(1) = 1$. Die Nullstelle $x = 0$ kann nicht mit Hensel geliftet werden, da $v_3(f(0)) = v_3(9) = 2$ aber $v_3(f'(0)) = v_3(f'(3)) = 1$. Auch modulo 9 bringt uns nicht weiter, also betrachten wir die Nullstellen modulo 27. Es ist

$$f(0) \equiv f(3) \equiv f(9) \equiv f(12) \equiv f(18) \equiv f(21) \equiv -9 \mod 27$$
$$f(6) \equiv f(15) \equiv f(24) \equiv 9 \mod 27$$

Also existieren keine Nullstellen modulo $27\mathbb{Z}_3$ und damit auch keine in $\mathbb{Z}_3$.

(d) Bereits über $\mathbb{Z}$ ist $f(X) = (X+1)(X^2 - X + 1)$. Also ist $-1 \in \mathbb{Z}_7$ eine Nullstelle. Das Polynom $g(X) := X^2 - X + 1$ besitzt in $\mathbb{F}_7$ die Nullstellen -2 und 3.

Sei nun $a_0 = 3$. Dann ist $d := v_7(g(a_0)) - 2v_7(g'(a_0)) = v_2(7) + 2v_2(5) = 1$. Also liftet a_0 zu einer Nullstelle $a \in \mathbb{Z}_7$ und nach Aufgabe 1c liefert a_3 die gesuchte Näherung. Es wird $a_1 = 8/5$, $a_2 = 39/55$ und $a_3 = -1504/1265$. Der Standardvertreter von $a_3 + 7^6\mathbb{Z}_7$ ist 34968.

Also liefert $34968 = 3 + 4 \cdot 7 + 6 \cdot 7^2 + 3 \cdot 7^3 + 0 \cdot 7^4 + 2 \cdot 7^5$ die ersten sechs Stellen von a in der Standarddarstellung.

Sei nun $b_0 = -2$. Dann ist $d := v_7(g(b_0)) - 2v_7(g'(b_0)) = v_2(7) + 2v_2(-5) = 1$. Also liftet b_0 zu einer Nullstelle $b \in \mathbb{Z}_7$ und nach Aufgabe 1c dürfen wir erneut nach der 3. Iteration abbrechen. Es wird $b_1 = -3/5$, $b_2 = 16/55$, $b_3 = 2769/1265$. Der Standardvertreter von $b_3 + 7^6\mathbb{Z}_7$ ist 82682.

Also liefert $82682 = 5 + 2 \cdot 7 + 0 \cdot 7^2 + 3 \cdot 7^3 + 6 \cdot 7^4 + 4 \cdot 7^5$ die ersten sechs Stellen von b in der Standarddarstellung.

(e) Sei $a_0 = 1$. Dann ist $d := v_3(f(a_0)) - 2v_3(f'(a_0)) = v_3(18) - 2v_3(4) = 2$. Also liftet a_0 zu einer Nullstelle $a \in \mathbb{Z}_3$ und nach Aufgabe 1c dürfen wir nach der 2. Iteration abbrechen.

Es wird $a_1 = -7/2$ und $a_2 = -362/115$. Der Standardvertreter von $a_2 + 3^6\mathbb{Z}_7$ ist 523.

Also liefert $523 = 1 + 0 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + 0 \cdot 3^4 + 2 \cdot 3^5$ die ersten sechs Stellen von a in der Standarddarstellung.

Sei $b_0 = 2$. Dann ist $d := v_3(f(b_0)) + 2v_3(f'(b_0)) = v_3(27) - v_3(15) = 3 - 2 = 1$. Also liftet b_0 zu einer Nullstelle $b \in \mathbb{Z}_3$ und nach Aufgabe 1c dürfen wir nach der 3. Iteration abbrechen.

Es wird $b_1 = 1/5$, $b_2 = 353/10$ und $b_3 = 14867174/634645$. Der Standardvertreter von $b_3 + 3^6\mathbb{Z}_7$ ist 497.

Also liefert $497 = 2 + 0 \cdot 3 + 1 \cdot 3^2 + 0 \cdot 3^3 + 0 \cdot 3^4 + 2 \cdot 3^5$ die ersten sechs Stellen von b in der Standarddarstellung.

Das Polynom $f(X)$ hat also mindestends zwei und damit sogar genau drei Nullstellen in $\mathbb{Q}_3$ bzw. $\mathbb{Z}_3$. Wegen $f(0) \equiv_3 1$ muß die dritte Nullstelle also ebenfalls kongruent zu ± 1 modulo 3 sein. Wir betrachten das Polynom also modulo 9 und finden:

Sei $c_0 = 5$. Dann ist $d := v_3(f(c_0)) + 2v_3(f'(c_0)) = v_3(162) - 2v_3(84) = 4 - 2 = 2$. Also liftet c_0 zu einer Nullstelle $c \in \mathbb{Z}_3$ und nach Aufgabe 1c dürfen wir nach der 2. Iteration abbrechen.

Es ist $c_1 = 43/14$ und $c_2 = 23042/15295$. Der Standardvertreter von $c_2 + 3^6\mathbb{Z}_7$ ist 437.

Also liefert $437 = 2 + 1 \cdot 3 + 0 \cdot 3^2 + 1 \cdot 3^3 + 2 \cdot 3^4 + 1 \cdot 3^5$ die ersten sechs Stellen von c in der Standarddarstellung.

Die drei Nullstellen unterscheiden sich bereits modulo 9, also sind sie verschieden.

Aufgabe 3.

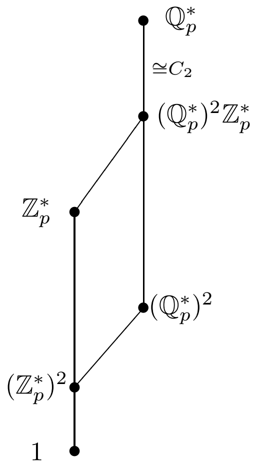
Klar ist, daß die gesuchten Gruppen elementar abelsche 2-Gruppen sind (sofern sie endlich sind).

Sei zunächst $p \neq 2$. Ist $x \in (\mathbb{Z}_p^*)^2$, so ist auch $x + p\mathbb{Z}_p^*$ ein Quadrat in $\mathbb{Z}_p^*/p\mathbb{Z}_p^* \cong \mathbb{F}_p^*$. Wir behaupten, daß auch die Umkehrung der Aussage gilt. Sei dazu $x \in \mathbb{Z}_p^*$ so, daß es ein $a_0 \in \mathbb{Z}_p$ gibt mit $x \equiv a_0^2 \mod p\mathbb{Z}_p$. Sicher ist dann $a_0 \notin p\mathbb{Z}_p$. Setzen wir $f(X) := X^2 - x$, so ist also $v_p(f(a_0)) \geq 1$ und $v_p(f'(a_0)) = v_p(2a_0) = 0$. Daher liftet a_0 zu einer Nullstelle $a \in \mathbb{Z}_p$ von f. Damit ist $a^2 = x$ und $a \in \mathbb{Z}_p^*$ wie behauptet.
Wir haben somit $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2 \cong \mathbb{F}_p^*/(\mathbb{F}_p^*)^2 \cong C_2$ gezeigt.

Sei nun $p = 2$. Wir setzen $R = \mathbb{Z}/8\mathbb{Z}$. Dann ist $(x + 8\mathbb{Z})^2 = 1 + 8\mathbb{Z}$ für alle $x \in \{1, 3, 5, 7\}$. Also ist $R^*/(R^*)^2 \cong C_2 \times C_2$ erzeugt von $(3 + 8\mathbb{Z})(R^*)^2$ und $(5 + 8\mathbb{Z})(R^*)^2$. Wieder ist klar, daß jedes $x \in (\mathbb{Z}_p^*)^2$ auch ein Quadrat modulo $8\mathbb{Z}_2$ ist und wir behaupten, daß auch die Umkehrung gilt. Sei

also $x \in \mathbb{Z}_2^*$ so, daß es ein $a_0 \in \mathbb{Z}_2$ gibt mit $x \equiv a_0^2 \mod 8\mathbb{Z}_2$. Sicher ist dann $a_0 \notin 2\mathbb{Z}_2$. Setzen wir $f(X) := X^2 - x$, so ist also $v_2(f(a_0)) \geq 3$ und $v_p(f'(a_0)) = v_p(2a_0) = 1$. Daher liftet a_0 zu einer Nullstelle $a \in \mathbb{Z}_2$ von f. Damit ist $a^2 = x$ und $a \in \mathbb{Z}_2^*$ wie behauptet.
Also ist $\mathbb{Z}_2^*/(\mathbb{Z}_2^*)^2 \cong R^*/(R^*)^2 \cong C_2 \times C_2$ und der kanonische Isomorphismus $\mathbb{Z}_2^*/(\mathbb{Z}_2^*)^2 \cong R^*/(R^*)^2$ bildet die Erzeuger $(3 + 8\mathbb{Z})(R^*)^2$ und $(5 + 8\mathbb{Z})(R^*)^2$ von $R^*/(R^*)^2$ ab auf $3(\mathbb{Z}_2^*)^2$ bzw. $5(\mathbb{Z}_2^*)^2$.

Jetzt zu $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ mit p beliebig. Wegen $v((\mathbb{Q}_p^*)^2) = 2\mathbb{Z}$ ist $(\mathbb{Q}_p^*)^2 \cap \mathbb{Z}_p^* = (\mathbb{Z}_p^*)^2$. Weiter ist $p \notin (\mathbb{Q}_p^*)^2\mathbb{Z}_p^*$ aber $p^2 \in (\mathbb{Q}_p^*)^2\mathbb{Z}_p^*$ und offensichtlich ist $\langle p, (\mathbb{Q}_p^*)^2, \mathbb{Z}_p^* \rangle = \mathbb{Q}_p^*$. Also haben wir folgende Situation:



Also ist $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \cong C_2 \times \mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2 \cong \begin{cases} C_2 \times C_2 & \text{falls } p \neq 2 \\ C_2 \times C_2 \times C_2 & \text{falls } p = 2 \end{cases}$ erzeugt von $p(\mathbb{Q}_p^*)^2$ sowie den $(\mathbb{Q}_p^*)^2$-Nebenklassen von Vertretern von $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2$.

Aufgabe 4.

Lemma Sei R ein kommutativer Ring. Dann ist $\mathrm{GL}_n(R) = \{x \in R^{n \times n} \mid \det(x) \in R^*\}$.
Beweis: Ist $x \in \mathrm{GL}_n(R)$ so existiert per Definition ein $y \in R^{n\times n}$ mit $xy = I_n$. Die Determinante ist multiplikativ, also $1 = \det(I_n) = \underbrace{\det(x)}_{\in R}\underbrace{\det(y)}_{\in R}$. Also ist $\det(x) \in R^*$.
Ist umgekehrt $x \in R^{n\times n}$ mit $\det(x) \in R^*$, so erfüllt die zu x adjunguierte Matrix $y \in R^{n\times n}$ die Identität $xy = \det(x)I_n$ also ist $x \in \mathrm{GL}_n(R)$.

Jetzt zur eigentlichen Aufgabe. Es ist

$$\begin{aligned}
(E, b) \text{ regulär} &\iff b_E \text{ ist bijektiv} \\
&\iff \text{für alle } a_1, \dots, a_n \in R \text{ existiert genau ein } x \in E \text{ mit } b(x, e_i) = a_i \text{ stets} \\
&\iff \text{für alle } a \in R^{1\times n} \text{ existiert genau ein } y \in R^{1\times n} \text{ mit } yG = a \\
&\iff G \in \mathrm{GL}_n(R) \\
&\iff \det(G) \in R^* \,.
\end{aligned}$$

Für ein ganzes Gitter L gilt also: L regulär $\iff \det(L) = 1$. Aber für ein ganzes Gitter ist die letzte Bedingung äquivalent zu $L = L^{\#}$.