Aufgabe 1

(i)

Da $\mathbb{F}_2$ ein Körper ist, ist $\mathbb{F}_2[x]$ ein Hauptidealring und somit $(f) \subset \mathbb{F}_2[x]$ ein maximales Ideal, da f irreduzibel ist. Daher ist der Quotient $R = \mathbb{F}_2[x]/(f)$ ein Körper

(ii)

Der Körper R ist ein 2-dimensionaler $\mathbb{F}_2$-Vektorraum (vgl. Bsp. 2.2.13) und besitzt somit 4 Elemente.

(iii)

R sieht nach Bsp. 2.2.13 so aus

+	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

·	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	$\bar{x}$

Bsp.:

$\bar{x} \cdot (\overline{x+1})$

$= \bar{x}^2 + \bar{x}$

$= \bar{f} = 0$ in R

$= -\bar{1}$

$= \bar{1}$ über $\mathbb{F}_2$

Aufgabe 2

(i)

Sei $f \in K[x]$ mit $\deg(f) = 3$.

"$\Rightarrow$":

Schreibe $f = gh$. Da f irreduzibel ist, muss $g \in K^\times$ oder $h \in K^\times$ gelten. O.E. gelte $g \in K^\times$. Dann ist also $\deg(h) = 3$ und es gibt keine Zerlegung von f in welcher ein Grad 1 Polynom auftritt.

"$\Leftarrow$":

Schreibe $f = gh$. Da f keine Wurzeln in K besitzt, muss $\deg(g) \neq 1 \neq \deg(h)$ gelten. Somit also $\deg(g) = 3$ und $\deg(h) = 0$ oder $\deg(g) = 0$ und $\deg(h) = 3$, sodass f irreduzibel ist.

(ii)

Gilt nicht mehr:

Betrachte z.B. das reduzible Polynom

$$f = x^4 + 2x^2 + 1 = \underbrace{(x^2+1)^2}_{\text{hat offenbar keine Nullstellen in } \mathbb{Q}} \in \mathbb{Q}[x].$$

Aufgabe 3

(i)

Wie in Aufgabe 1 gesehen, ist

$\mathbb{F}_2 \hookrightarrow \mathbb{F}_2[x]/(x^2+x+1)$

eine Körpererweiterung von Grad 2.

(ii)

Offenbar sind $\pm\bar{1} \in \ker(\varphi)$. Da die Elemente des Kernes von φ genau aus den Elementen $x \in \mathbb{F}_p^\times$ bestehen mit $x^2 = 1$ (also $x^2 - 1 = 0$), kann es außerdem höchstens zwei solche Elemente geben. (das Polynom x^2-1 hat maximal zwei Nullstellen). Somit erhalten wir also $\ker(\varphi) = \{\pm\bar{1}\}$. Daher ist φ nicht injektiv und somit auch nicht surjektiv (Definitions- und Zielbereich sind endlich und gleich mächtig). Also ist M nicht leer.

Nach den Isomorphiesatz erhalten wir nun

$\frac{p-1}{2} = \frac{|\mathbb{F}_p^\times|}{2}$ viele Quadrate in $\mathbb{F}_p^\times$ und somit

$\frac{p+1}{2}$ Quadrate in $\mathbb{F}_p$, da $0 = 0^2$ stets ein Quadrat ist. Daher gibt es $p - \frac{p+1}{2} = \frac{p-1}{2}$ Elemente in $\mathbb{F}_p$, welche keine Quadrate sind.

(iii)

Sei $a \in M$. Dann ist $x^2 - a \in \mathbb{F}_p(x)$ irreduzibel, da a kein Quadrat ist und somit $x^2 - a$ keine Nullstellen (in $\mathbb{F}_p$) hat. Wir erhalten also durch

$\mathbb{F}_p \hookrightarrow \mathbb{F}_p[x]/(x^2-a)$

eine Körpererweiterung von Grad 2.

Aufgabe 4

Für jeden Ring R ist

$\varphi: R(x) \to R(x),\ f(x) \mapsto f(x+1)$

ein Automorphismus von Ringen mit Umkehrabbildung $g(x) \mapsto g(x-1)$. Da Ringhomomorphismen Produkte und Einheiten respektieren überträgt sich also auch Irreduzibilität entlang φ bzw. φ^{-1}.

Es ist

$\Phi_p(x[redacted])(x-1) = x^p - 1$

und somit

$$\Phi_p(x) = \frac{x^p - 1}{x - 1}.$$

Daher erhalten wir

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{(x+1)^p - 1}{x}$$

$$= \frac{\left(\sum_{j=0}^{p} \binom{p}{j} x^j\right) - 1}{x}$$

$$= \frac{\sum_{j=1}^{p} \binom{p}{j} x^j}{x}$$

$$= [redacted] \sum_{j=1}^{p} \binom{p}{j} x^{j-1}$$

$$= \sum_{j=0}^{p-1} \binom{p}{j+1} x^j$$

für $j \neq p-1$ stets durch p teilbar und für $j = 0$ nicht durch p^2 teilbar

Also ist $\Phi_p(x+1)$ [redacted] nach Eisenstein irreduzibel und somit auch $\Phi_p(x)$.