2.5.6 Lemma R Intring. Dann $p \in R$ prim $\Rightarrow p \in R[X]$ prim

Beweis Dasselbe Argument wie in 2.5.5. ▤

2.5.7 Lemma R faktoriell, $a \in R \setminus \{0\}$, $f, g \in R[X]$ mit g primitiv. Gilt $g \mid af$, so $g \mid f$

Beweis $g \mid af \Rightarrow \exists g' : af = gg' \Rightarrow c(af) = c(gg')$

$\overset{2.5.5}{\Rightarrow} a\,c(f) = \underbrace{c(g)}_{=1}\, c(g') \Rightarrow a\,c(f) = c(g') \Rightarrow$

$af = g\,c(g')g'' = g\,a\,c(f)g'' \Rightarrow f = g\,c(f)g'' \Rightarrow g \mid f$ ▤

2.5.8 Lemma R faktoriell. Dann gilt für $f \in R[X]$, $\operatorname{grad} f \geq 1$:

(a) f irred in $R[X]$

(b) f primitiv und irred. in $K[X]$, $K = Q(R)$

Beweis (a) $\Rightarrow$ (b) f irred $\Rightarrow f$ primitiv ✓. Angenommen f reduzibel in $K[X]$ d.h. $f = gh$, $1 \leq \operatorname{grad} g < \operatorname{grad} f$; $g, h \in K[X]$

$\rightsquigarrow \exists a \in R$ mit $af = g'h'$ mit $g', h' \in R[X]$. Sei $g' = c(g')g''$

$\overset{2.5.7}{\rightsquigarrow} g'' \mid f$ ↯ ▤

2.5.9 Lemma R faktoriell. Dann $f \in R[X]$ irred $\Rightarrow f$ prim.

Beweis $\operatorname{grad} f = 0 \rightsquigarrow f \in R$ irred $\rightsquigarrow f$ prim in $R \overset{2.5.6}{\rightsquigarrow} f$ prim in $R[X]$

Sei $\operatorname{grad} f > 0 \rightsquigarrow f$ primitiv. Sei $f \mid gh \overset{2.5.8}{\rightsquigarrow} f \mid g$ in $K[X]$ OBdA

$\rightsquigarrow g = ff'$, $f' \in K[X] \rightsquigarrow \exists a \in R$ $af' \in R[X]$

Weil $ag = f(af') \rightarrow f \mid ag \overset{2.5.7}{\rightsquigarrow} f \mid g$ in $R[X]$ ▤

Beweis des Satzes von Gauss 2.5.1.

Wegen Lemma 2.5.9 genügt es zu zeigen, dass jedes $f \in R[X]$, $f \neq 0$, $f \notin R^*$ eine Darstellung als Prod. von irred. Elem. besitzt.

Induktion nach grad f. Ist grad f = 0, so ist $f \in R \rightsquigarrow$ f ist Prod. von irred. (≡ prim) Elem., da R faktoriell.
Ist grad f > 1, so gilt $f = c(f) f^*$ mit f^* primitiv.
Ist f^* irred. so ist die Aussage wahr. Ist $f^* = gh$ mit grad g, grad h < grad f^* so kann man die Induktionsvoraussetzung anwenden. ▤

2.5.10 Satz (Eisensteinsches Kriterium)
Sei R faktoriell, $f = a_n X^n + \dots + a_0 \in R[X]$, $n > 0$, primitiv.
Ist $p \in R$ prim, $p \nmid a_n$, $p \mid a_i$ für $0 \le i < n$, $p^2 \nmid a_0$
so ist f irred. in $R[X]$.

Beweis Sei $f = g \cdot h$ mit $g = \sum_{i=0}^{r} b_i X^i$, $h = \sum_{j=0}^{s} c_j X^j$
mit $g, h \notin R^*$. Dann $g, h \notin R$ (da f primitiv), also $r, s > 0$.
Damit $a_n = b_r c_s$ und $p \nmid b_r$, $p \nmid c_s$. Außerdem $a_0 = b_0 c_0$
und $p \mid b_0 c_0$, $p^2 \nmid b_0 c_0$. OBdA $p \mid b_0$, $p \nmid c_0$.
Sei $t = \max\{j : p \mid b_j\}$, also $0 \le t < r$. Dann gilt

$$a_{t+1} = \underbrace{b_0 c_{t+1} + \dots + b_t c_1}_{\text{teilbar durch } p} + \underbrace{b_{t+1} c_0}_{\text{nicht teilbar durch } p} \Rightarrow p \nmid a_{t+1}$$

$$\Rightarrow n = \underbrace{t+1}_{<r \ \le s} < r + s = n \quad \lightning \quad ▤$$

2.5.11 Bsp. $f = X^{p-1} + X^{p-2} + \dots + X + 1$ ist irred. in $\mathbb{Z}[X]$,
für p prim. Es reicht zu zeigen, dass $f(X+1)$ irred ist.
Aber
$$f(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = \frac{X^p + \binom{p}{1} X^{p-1} + \dots + \binom{p}{p-1} X}{X}$$
$$= X^{p-1} + \binom{p}{1} X^{p-2} + \dots + \binom{p}{p-2} X + \underbrace{\binom{p}{p-1}}_{=p}$$

Aber $p \mid \binom{p}{k} = \frac{p!}{k!(p-k)!}$, $1 \le k \le p-1$ und $p \not\equiv 0 \pmod{p^2}$

Eisenstein $\rightsquigarrow$ $f(X+1)$ irred.

3. Körpererweiterungen

§ 3.1. Die Charakteristik eines Körpers

3.1.1 Def. Sei K ein Körper. (i) Betrachte den Ringhomom $\varphi: \mathbb{Z} \to K$ definiert durch $\varphi(1)=1$ mit $\ker\varphi = p\mathbb{Z}$, $p \in \mathbb{N}_0$. Dann heißt $\operatorname{char} K := p$ die Charakteristik von K.

(ii) Ein Unterring T von K, der Körper ist, heißt Teilkörper von K.

(iii) Der Durchschnitt aller Körper von K ist Körper und heißt Primkörper von K.

3.1.2 Satz (i) $T \subset K$ Teilkörper $\Rightarrow \operatorname{char} T = \operatorname{char} K$.

(ii) $\operatorname{char} K$ ist 0 oder prim

(iii) Sei P der Primkörper von K. Dann: $\operatorname{char} P = 0 \Leftrightarrow P \cong \mathbb{Q}$
$\operatorname{char} P = p > 0 \Leftrightarrow P = \mathbb{Z}/p\mathbb{Z}$. In jedem Falle gilt $P \cong \mathbb{Q}(\operatorname{Im}\varphi)$ für obiges φ.

Beweis (i) $1 \in T$ also $\operatorname{Im}\varphi \subset T$

(ii) $\mathbb{Z}/\ker\varphi \cong \operatorname{Im}\varphi \subset K$; K Körper $\Rightarrow \operatorname{Im}\varphi$ Int.ring $\Rightarrow \ker\varphi$ primideal

(iii) Es ist klar, dass $P \cong \mathbb{Q}(\operatorname{Im}\varphi)$ da $\operatorname{Im}\varphi \subset T$ für alle Teilkörper T von K. Ist $\operatorname{char} K = 0 \Rightarrow \mathbb{Z} \cong \operatorname{Im}\varphi$ also $\mathbb{Q} = \mathbb{Q}(\mathbb{Z}) \cong \mathbb{Q}(\operatorname{Im}\varphi) \cong P$. Ist $\operatorname{char} K = p > 0$, so ist $\mathbb{Z}/p\mathbb{Z} \cong \operatorname{Im}\varphi$ Körper, also $P \cong \mathbb{Q}(\operatorname{Im}\varphi) \cong \operatorname{Im}\varphi \cong \mathbb{Z}/p\mathbb{Z}$. ∎

§ 3.2. Endliche und algebraische Körpererweiterungen.

3.2.1 Bem. Ist L Körper, $K \subset L$ Teilkörper, so ist L ein K-VR.

3.2.2 Def. (i) Eine Körpererweiterung ist ein Paar $K \subset L$, mit L Körper und K Teilkörper.