Übung zu Algebraische und Geometrische Strukturen in der Mathematik, SoSe 2014

5. Übungsblatt – Lösungsskizze

Aufgabe P14

Wir haben
$$(X^{\alpha-1} + X^{\alpha-2} + ... + X + 1)(X + 1) = X^{\alpha} - 1,$$
also können wir symbolisch auch
$$X^{\alpha-1} + X^{\alpha-2} + ... + X + 1 = \frac{X^{\alpha} - 1}{X - 1}$$
schreiben. Falls $\alpha = 2n$, so gilt $X^{\alpha} - 1 = (X^n + 1)(X^n - 1)$, also
$$(X^{\alpha-1} + X^{\alpha-2} + ... + X + 1)(X - 1) = (X^n + 1) \cdot (X^n - 1).$$
Damit hat $X^{\alpha-1} + X^{\alpha-2} + ... + X + 1$ eine Nullstelle bei -1 und ist folglich nicht irreduzibel.

Aufgabe P15

Wir beobachten zunächst, dass $m_{a,k} = m_{b,k}$ gilt (warum?). Aus Aufgabe P12 erhalten wir somit einen Isomorphismus
$$k(a) \to k[X]/(m_{a,k} \cdot k[X]) = k[X]/(m_{b,k} \cdot k[X]) \to k(b),$$
der nach der dortigen Konstruktion a auf b abbildet und auf k die Identität ist.

Aufgabe P16

Sei $F \subseteq E$ der Primkörper. Dann ist $F \subseteq E$ insbesondere ein Teilkörper und es muss $[E : F]$ ein Teiler von $|E|$ sein, da $|E| = |F| \cdot [E : F]$ im Falle einer endlichen Erweiterung eines endlichen Körpers gilt (warum?). Da 27 nur den Teiler 3 hat muss also $F = \mathbb{Z}_3$ gelten. Um E ensprechend zu konstruieren reicht es also aus, ein normiertes und irreduzibles Polynom über $\mathbb{Z}_3$ mit Grad 2 und Grad 3 anzugeben. Wir können hierfür und $X^2 + 1$ und $X^3 + 2X + 1$ nehmen.

Aufgabe H12

Das Polynom Ψ_4 hat -1 als Nullstelle und es gilt
$$\Psi_4(X) = (X + 1)(X^2 + 1).$$
Da $X + 1$ und $X^2 + 1$ irreduzibel in $\mathbb{Q}[X]$ sind ist dies bereits die gewünschte Zerlegung. Damit gilt $\Phi_4(X) = X^2 + 1$, da $(X + 1)$ nicht $e^{\frac{2\pi i}{4}} = i$ als Nullstelle hat.
Das Polynom Ψ_6 hat ebenfalls -1 als Nullstelle und es gilt
$$\Psi_6(X) = (X + 1)(X^4 + X^2 + 1).$$
Durch einen Koeffizientenvergleich kann man eine Zerlegung von $(X^4 + X^2 + 1)$ konstruktiv raten und erhält
$$(X^4 + X^2 + 1) = (X^2 + X + 1)(X^2 - X + 1).$$

Damit gilt

$$\Psi_6(X) = (X+1)(X^2+X+1)(X^2-X+1),$$

wobei alle Faktoren irreduzibel sind (die letzten beiden z.B. nach dem Nullstellenkriterium). Außerdem haben wir

$$\Phi_4(X) = X^2 - X + 1,$$

da $1 + (e^{\frac{2\pi i}{6}})^2 = e^{\frac{2\pi i}{6}}$ gilt, wie man sich anhand eines in den Einheiskreis einbeschriebenen regelmäßigen 6-Ecks leicht klar macht.

Aufgabe H13

1. Gilt $p = s \cdot t$, so muss $\deg(s) = \deg(t) = 2$ oder $\deg(s) = 3$, $\deg(t) = 1$ oder $\deg(s) = 3$, $\deg(t) = 1$ gelten. Die letzten beiden Möglichkeiten sind dabei aus Symmetriegründen äquivalent. Setzt man die entsprechenden Polynome in $\mathbb{Z}_2[X]$ an und macht einen Koeffizientenvergleich, so sieht man, dass es in $\mathbb{Z}_2[X]$ keine solche Zerlegung geben kann. Im erster Fall hat man z.B.

   $$s(X) = X^2 + aX + b \text{ und } t(X) = cX^2 + d$$

   und durch $s \cdot t = p$ ergibt sich das LGS

   $$a + c = 0, \quad ac + b + d = 1, \quad ad + bc = 1, \quad bd = 0,$$

   welches über $\mathbb{Z}_2$ keine Lösung hat. Nach dem Reduktionskriterium ist damit auch p in $\mathbb{Q}[X]$ irreduzibel.

2. In $\mathbb{C}$ zerfällt p in Linearfaktoren. Außerdem treten die Nullstellen als Paare von komplex konjuguerten Zahlen auf, also

   $$p(X) = (X - z)(X - \overline{z})(X - w)(X - \overline{w})$$

   Koeffizientenvergleich mit p leifert dann alle 4 Identitäten.

3. Da z Nullstelle von p ist und p normiert und irreduzibel ist, gilt $p = m_{z,\mathbb{Q}}$ und $[\mathbb{Q}(z) : \mathbb{Q}] = \deg(m_{z,\mathbb{Q}}) = 4$.

4. Aus a) folgt $z + \overline{z} = -(w + \overline{w})$ und damit aus b) $z\overline{z} + w\overline{w} - (z + \overline{z})^2 = 0$.

5. Dies sieht man durch einen Widerspruchsbeweis: wäre z ein Element von $\triangle\mathbb{Q}$, dann auch $(z + \overline{z})^2$. Da $(z + \overline{z})^2$ Nullstelle des irreduziblen (nach Reduktionskriterium bzgl. $\mathbb{Z}_3$) und normierten Polynoms q ist gilt

   $$[\mathbb{Q}((z + \overline{z})^2) : \mathbb{Q}] = \deg(q) = 3,$$

   was keine Potenz von 2 ist. Also kann nicht $z \in \triangle\mathbb{Q}$ gelten.