1. Seien R ein kommutativer Ring mit 1 und $X_1, \ldots, X_n$ Unbestimmte über R. Für $0 \leq k \leq n$ definiere das k-te elementarsymmetrische Polynom als

$$s_k = \sum_{\substack{J \subseteq \{1,\ldots,n\} \\ |J|=k}} \prod_{j \in J} X_j.$$

Beispielsweise gilt also für $n = 3$

$$s_0 = 1, \qquad s_1 = X_1 + X_2 + X_3, \qquad s_2 = X_1X_2 + X_1X_3 + X_2X_3, \qquad s_3 = X_1X_2X_3.$$

Ein Polynom $f \in R[X_1, \ldots, X_n]$ heißt *symmetrisch*, wenn

$$F(X_{\sigma(1)}, X_{\sigma(2)} \ldots, X_{\sigma(n)}) = F(X_1, X_2, \ldots, X_n)$$

für alle Permutationen $\sigma \in S_n$ gilt.
Weiters setze $P_k = \sum_{j=1}^n X_j^k$.

   (a) Zerlegen Sie $\sum_{j=0}^n (-1)^{n-j} s_{n-j} Z^j$ in Linearfaktoren.

   (b) Es gilt $P_2 = s_1^2 - 2s_2$ (Check!). Stellen Sie P_3 durch s_1, s_2 und s_3 dar.

   (c) Die Folge P_k, $k \in \mathbb{N}_0$, erfüllt eine Rekursionsgleichung n-ter Ordnung. Welche?

   (d) Zeigen Sie: $\{f \in R[X_1, \ldots, X_n] : f \text{ ist symmetrisch}\} = R[s_1, s_2, \ldots, s_n]$, d.h., jedes symmetrische Polynom ist als Polynom allein in den elementarsymmetrischen Polynomen darstellbar (so wie die Beispiele in Teil 2).
   Hinweis. Sortieren Sie die Summanden von $f = \sum c_{\alpha_1,\ldots,\alpha_n} X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ lexikographisch absteigend nach $(\alpha_1, \ldots, \alpha_n)$.

2. Seien M/L und L/K endliche Körpererweiterungen und $\beta \in M$. Zeigen Sie

$$N_{L/K}(N_{M/L}(\beta)) = N_{M/K}(\beta).$$

Hinweis. Betrachten Sie zunächst den Fall $M = L(\beta)$. Hier ist es günstig, $\{1, \beta, \ldots, \beta^{m-1}\}$ als Basis von M/L zu wählen, wobei $m = [L(\beta) : L]$.

3. Sei $L = \mathbb{Q}(\sqrt{2007}, \sqrt{3}, \sqrt{6})$. Bestimmen Sie den Grad von L über $\mathbb{Q}$, alle $\mathbb{Q}$-Homomorphismen von L nach $\mathbb{C}$, ein primitives Element der Körpererweiterung $L/\mathbb{Q}$. Drücken Sie die angegebenen Erzeuger durch das primitive Element aus.

4. Berechnen Sie $\beta = 1/(\alpha^2 + 7)$ (als Linearkombination von $1, \alpha, \alpha^2$), wobei $\alpha^3 + 2007\alpha^2 + 3\alpha + 6 = 0$. Berechnen Sie auch das Minimalpolynom von β sowie numerische Näherungen seiner absoluten und relativen Konjugierten.

5. Besorgen Sie das Programmpaket PARI/GP. Lösen Sie damit Beispiel 4.

6. Sei K ein Körper der Charakteristik $p > 0$, X eine Unbestimmte über K und $L = K(X)$ der Körper der rationalen Funktionen in X mit Koeffizienten aus K. Zeigen Sie, dass das Polynom $f(Z) = Z^p - X$ aus $L[Z]$ irreduzibel, aber nicht separabel ist.

7. Sei L/K eine endliche separable Körpererweiterung und φ eine lineare Funktion auf dem Vektorraum L über K mit Werten aus K. Zeigen Sie, dass es dann genau ein $\beta \in L$ gibt, sodass für alle $x \in K$ die Beziehung $\varphi(x) = \mathrm{Tr}_{L/K}(\beta x)$ gilt.

8. Sei D eine quadratfreie ganze Zahl (d.h., es gebe kein $a \in \mathbb{Z}$ mit $a^2 \mid D$). Bestimmen Sie alle Zahlen in $\mathbb{Q}(\sqrt{D})$, die ganz über $\mathbb{Z}$ sind.

9. Sei V ein n-dimensionaler K-Vektorraum, $F : V \to V$ linear. Betrachte V als $K[X]$-Modul mit
$$\left(\sum_{j=0}^{n} a_j X^j\right) v = \sum_{j=0}^{n} a_j F^j(v), \qquad v \in V.$$
   (a) Zeigen Sie, dass V ein endlich erzeugter $K[X]$-Modul ist.
   (b) Benutzen Sie den Struktursatz für endlich erzeugte Moduln über Hauptidealbereichen, um zu zeigen, dass
   $$V \simeq K/(f_1^{e_1}) \oplus \cdots \oplus K/(f_r^{e_r})$$
   für (nicht notwendig verschiedene) irreduzible Polynome f_j, $j \in \{1, \ldots, r\}$ und natürliche Zahlen e_j gilt.
   (c) Geben Sie eine Matrixdarstellung von F bezüglich einer mit der Zerlegung in 9b verträglichen Basis von V an.
   (d) Wie vereinfacht sich die Zerlegung in 9b, wenn K algebraisch abgeschlossen ist?
   (e) Wie sieht die Matrixdarstellung von F in diesem Fall aus?
   (f) Zeigen Sie: es gibt genau dann ein $v \in V$, sodass $v, F(v), \ldots, F^{n-1}(v)$ linear unabhängig sind, wenn die irreduziblen Polynome in der Darstellung von 9b paarweise verschieden sind.

10. Besorgen Sie das Programmpaket KANT/KASH. Lösen Sie damit Beispiel 4

11. Sei $f \in \mathbb{Z}[X]$.
   (a) Sei f normiert. Geben Sie ein (ineffizientes) Verfahren an, f in $\mathbb{Z}[X]$ zu faktorisieren, indem Sie alle komplexen Nullstellen näherungsweise bestimmen und damit auf Faktorensuche gehen, wobei Sie Eigenschaften ganzalgebraischer Zahlen ausnutzen. Faktorisieren Sie damit $f = (X^2 - 256)(X^2 - 1)X - 1$.
   (b) Wie kann man obiges Verfahren auch verwenden, wenn der Leitkoeffizient nicht 1 ist. Erproben Sie das an $17X^5 + 25X^2 + 3$.

12. Verallgemeinern Sie die Idee aus Beispiel 11 zu einer weiteren Lösung von Beispiel 3.

13. Bestimmen Sie eine Ganzheitsbasis von $\mathbb{Q}(\alpha)$, wobei α eine Nullstelle von
   (a) $f = (X^2 - 25)X(X^2 - 1) - 1$
   (b) $f = X^4 - 80X^3 - X^2 + 80X - 1$

   ist. Verwenden Sie zunächst keine spezialisierte Software (also ein „gewöhnliches“ Computeralgebrasystem). Bestimmen Sie jeweils auch die Diskriminante des Körpers sowie die Diskriminante der mit dem jeweils angegebenen Gleichungsordnung.

14. Beispiel 13 mit Pari.

15. Beispiel 13 mit Kant.

16. Geben Sie ein (oder mehrere) Beispiel eines Ringes R, einer multiplikativ abgeschlossenen Teilmenge D von R sowie zwei Idealen I und J an, sodass $D^{-1}I = D^{-1}J$.

17. Seien ω_1, ω_2, ω_3 linear unabhängige Zahlen eines algebraischen Zahlkörpers K. Man zeige, dass
$$\{a\omega_1 + b\omega_2 + c\omega_3 : a, b, c \in \mathbb{Z}, 2a + 3b + 5c = 0\}$$
ein freier $\mathbb{Z}$-Modul ist, und gebe eine Basis an.

18. Man bestimme die Dedekindsche Ordnung von $\langle 2, \sqrt{2}/2\rangle$ in $\mathbb{Q}(\sqrt{2})$.

19. Man zeige, dass es in $\mathbb{Q}$ eine einzige Ordnung gibt, nämlich den Ring der ganzen Zahlen.

20. Zeigen Sie, dass der Durchschnitt zweier vollständiger Gitter in einem Zahlkörper wieder ein vollständiges Gitter ist.

21. Sei M ein vollständiges Gitter in einem algebraischen Zahlkörper K.

    (a) Man zeige, dass
    $$M^* := \{\xi \in K : \forall \alpha \in M \, \mathrm{Tr}(\alpha\xi) \in \mathbb{Z}\}$$
    ebenfalls ein vollständiges Gitter von K (das komplementäre Gitter von M) ist.

    (b) Man zeige $(M^*)^* = M$, d.h. das komplementäre Gitter von M^* ist M.

    (c) Man zeige, dass die komplementären Gitter M und M^* dieselbe Dedekindsche Ordnung haben.

    (d) Man zeige, dass für vollständige Gitter M_1 und M_2 die Beziehungen $M_1 \subseteq M_2$ und $M_1^* \supseteq M_2^*$ äquivalent sind.

22. Bestimmen Sie alle Primideale in $\mathfrak{o}_{\mathbb{Q}(\sqrt{-7})}$, die über dem Primideal $2\mathbb{Z}$ von $\mathbb{Z}$ liegen.

23. Quadratische Zahlkörper sind durch ihre Diskriminante eindeutig bestimmt. Für kubische Zahlkörper gilt das nicht mehr: Betrachten Sie die Zahlkörper, die durch Adjunktion von Nullstellen der Polynome

$$X^3 - 18X - 6, \qquad X^3 - 36X - 78, \qquad X^3 - 54X - 150$$

zu $\mathbb{Q}$ entstehen. Bestimmen Sie deren Diskriminanten. Zeigen Sie deren Nicht-Isomorphie durch Betrachtung der Primzerlegung von 5 und von 13 in den jeweiligen Ganzheitsringen.

24. Bestimmen Sie den Zerfällungskörper von

$$X^3 + X^2 - 2X - 1$$

über $\mathbb{Q}$.

25. Zeigen Sie: Falls $f \in \mathbb{Z}[X]$ ein kubisches Polynom mit einer nicht-reellen Nullstelle ist, so hat der Zerfällungskörper von f über $\mathbb{Q}$ stets Grad 6 über $\mathbb{Q}$.

26. Sei α eine nicht-reelle Nullstelle von $X^3 + X^2 - 1$.

    (a) Bestimmen Sie das Minimalpolynom von $\alpha\overline{\alpha}$, wobei $\overline{\alpha}$ aus α durch komplexe Konjugation entsteht.

    (b) Bestimmen Sie das Minimalpolynom von $\alpha/|\alpha|$.

    (c) Ist $\alpha/|\alpha|$ eine Einheitswurzel?

27. Sei f ein „Eisenstein“-Polynom modulo p (d.h., f und p erfüllen die Voraussetzungen des Eisensteinschen Irreduzibilitätskriteriums), α eine Nullstelle von f und $K = \mathbb{Q}(\alpha)$. Zeigen Sie, dass p den Index der Gleichungsordnung $\mathbb{Z}[\alpha]$ im Ganzheitsring von K nicht teilt.

28. Sei I ein Ideal des Ganzheitsringes eines algebraischen Zahlkörpers. Zeigen Sie, dass die Absolutnorm $\mathbf{N}(I)$ ein Element von I ist.

29. Sei R ein Dedekindring und I ein Ideal von R, $I \neq R$. Zeigen Sie:

    (a) Es gibt ein $\alpha \in R$, sodass das Hauptideal αR eine Faktorisierung $\alpha R = IJ_1$ für ein zu I teilerfremdes Ideal J_2 hat.

    (b) Es gibt ein $\beta \in R$, sodass das Hauptideal βR eine Faktorisierung $\beta R = IJ_2$ für ein zu J_1 teilerfremdes Ideal J_2 besitzt.

    (c) Es gilt $I = \alpha R + \beta R$.

    Jedes Ideal von R ist daher Hauptideal oder wird von zwei Elementen erzeugt.

30. Man bestimme alle Einheitswurzeln, die in einem algebraischen Zahlkörper vom Grad 4 enthalten sein können.

31. Sei K ein algebraischer Zahlkörper, der mindestens eine reelle Einbettung besitzt (i.e., $s \neq 0$). Zeigen Sie, dass die Gruppe der Einheitswurzeln von K genau zwei Elemente besitzt.

32. Der algebraische Zahlkörper K besitze eine komplexe Einheitswurzel. Man zeige, dass die Norm einer beliebigen Zahl $\beta \in K \setminus \{0\}$ positiv ist.