Aufgabe 1

Sei M eine Menge. Zur Definition der symmetrischen Differenz zweier Teilmengen von M siehe Aufgabenstellung.

Vorüberlegung: Für $X, Y, Z \subseteq M$ gilt:

$$\begin{aligned} & (X \cup Y) \backslash Z \\ = \; & \{m \in M : (m \in X \vee m \in Y) \wedge m \notin Z\} \\ = \; & \{m \in M : m \in X \wedge m \notin Z\} \cup \{m \in M : m \in Y \wedge m \notin Z\} \\ = \; & (X \backslash Z) \cup (Y \backslash Z) \end{aligned}$$

Und ebenso gilt:

$$\begin{aligned} & Z \backslash (X \cup Y) \\ = \; & \{m \in M : m \in Z \wedge m \notin (X \cup Y)\} \\ = \; & \{m \in M : m \in Z \wedge m \notin X \wedge m \notin Y\} \\ = \; & \{m \in M : m \in Z \wedge m \notin X\} \cap \{m \in M : m \in Z \wedge m \notin Y\} \\ = \; & (Z \backslash X) \cap (Z \backslash Y) \end{aligned}$$

Eine weitere Regel für Differenzen von Mengen lautet:

$$\begin{aligned} & (X \backslash Y) \backslash Z \\ = \; & \{m \in M : m \in X \wedge m \notin Y \wedge m \notin Z\} \\ = \; & \{m \in M : m \in X \wedge m \notin Z \wedge m \notin Y\} \\ = \; & (X \backslash Z) \backslash Y \end{aligned}$$

Nach diesen Gleichungen widmen wir uns nun der Aufgabe. Zu zeigen: $(\mathcal{P}(M), \Delta)$ ist eine kommutative Gruppe (eine solche Gruppe wird auch "abelsch" genannt).
Zunächst stellt man fest, dass offensichtlich $A \Delta B = B \Delta A$ für alle $A, B \subseteq M$ gilt.

(i) **Assoziativität**
Seien $A, B, C \subseteq M$.
Zu zeigen: $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.
Vereinfachen wir erst die linke Seite:

$$\begin{aligned} (A \Delta B) \Delta C &= ((A \backslash B) \cup (B \backslash A)) \Delta C \\ &= ((A \backslash B) \cup (B \backslash A)) \backslash C \cup C \backslash ((A \backslash B) \cup (B \backslash A)) \\ &= (A \backslash B) \backslash C \cup (B \backslash A) \backslash C \cup \underbrace{(C \backslash (A \backslash B) \cap C \backslash (B \backslash A))}_{=:D} \end{aligned}$$

Schauen wir uns die Menge D nochmal an:

$$\begin{aligned} D &= \{m \in M : m \in C \wedge m \notin (A \backslash B) \wedge m \notin (B \backslash A)\} \\ &= \{m \in M : m \in C \wedge (m \in (A \cap B) \vee m \notin (A \cup B)\} \\ &= (A \cap B \cap C) \cup \{m \in M : m \in C \wedge m \notin (A \cup B)\} \\ &= (A \cap B \cap C) \cup (C \backslash B) \backslash A \end{aligned}$$

Insgesamt also:

$$(A\Delta B)\Delta C = (A \cap B \cap C) \cup (C\backslash B)\backslash A \cup (A\backslash B)\backslash C \cup (B\backslash A)\backslash C$$

Anschaulich liegen also diejenigen Elemente von M in $(A\Delta B)\Delta C$, die in allen 3 Mengen liegen oder aber in genau einer.
Nun zur rechten Seite:

$$\begin{aligned} A\Delta(B\Delta C) &= A\Delta((B\backslash C) \cup (C\backslash B)) \\ &= A\backslash((B\backslash C) \cup (C\backslash B)) \cup ((B\backslash C) \cup (C\backslash B))\backslash A \\ &= \underbrace{(A\backslash(B\backslash C) \cap A\backslash(C\backslash B))}_{=:E} \cup (B\backslash C)\backslash A \cup (C\backslash B)\backslash A \end{aligned}$$

Genau wie oben ergibt sich:

$$E = (A \cap B \cap C) \cup (A\backslash B)\backslash C$$

Insgesamt folgt das Gewünschte.

(ii) **Neutrales Element**
Sei $A \subseteq M$ beliebig. Wir müssen die Existenz einer Menge $X \subseteq M$ zeigen mit der Eigenschaft:

$$A\Delta X = X\Delta A = A$$

Definiere nun $X := \emptyset$. Es gilt:

$$A\Delta\emptyset = (A\backslash\emptyset) \cup (\emptyset\backslash A) = A \cup \emptyset = A$$

Damit ist die leere Menge $\emptyset$ das gesuchte neutrale Element. Da wir die Kommutativität schon nachgewiesen haben, genügt es, nur diesen Fall zu betrachten.

(iii) **Inverses Element**
Sei wieder $A \subseteq M$ beliebig. Nun müssen wir die Existenz einer Menge A^{-1} zeigen mit der Eigenschaft:

$$A\Delta A^{-1} = A^{-1}\Delta A = \emptyset$$

Definiere $A^{-1} := A$. Dann gilt:

$$A\Delta A = (A\backslash A) \cup (A\backslash A) = \emptyset \cup \emptyset = \emptyset$$

Alle Gesetze einer Gruppe sind damit nachgewiesen. □

Aufgabe 2

Definiere $U := \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

(a) Zunächst gilt: $0 = 0 + 0 \cdot \sqrt{2} \in U$ und auch $1 = 1 + 0 \cdot \sqrt{2} \in U$. Für einen Unterring brauchen wir nun die Abgeschlossenheit von U bzgl. der Operationen $+$ und $\cdot$ in $\mathbb{R}$ und zu jedem $u \in U$ ein additives Inverses,

damit $(U, +)$ eine Gruppe wird.
Seien also $a + b\sqrt{2}$ und $c + d\sqrt{2}$ in U. (Also $a, b, c, d \in \mathbb{Q}$). Dann gilt:

$$\begin{aligned}(a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a + c) + (b + d)\sqrt{2} \in U \\ (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) &= ac + ad\sqrt{2} + bc\sqrt{2} + bd(\sqrt{2})^2 \\ &= (ac + 2bd) + (ad + bc)\sqrt{2} \in U\end{aligned}$$

Außerdem ist natürlich $(-a) + (-b)\sqrt{2} \in U$ und das ist bzgl. $+$ invers zu $a + b\sqrt{2}$. Damit ist U tatsächlich ein Unterring von $\mathbb{R}$.

(b) Es genügt zu zeigen, dass U abgeschlossen ist bzgl. der Bildung von Inversen bzgl. der Verknüpfung $\cdot$. Denn nach (a) ist U bereits ein Ring. Zunächst folgende Behauptung für $a, b \in \mathbb{Q}$:

$$a + b\sqrt{2} \neq 0 \Rightarrow a^2 - 2b^2 \neq 0$$

Angenommen es gilt $b = 0$. Dann ist aber nach Voraussetzung $a \neq 0$ und damit auch $a^2 \neq 0$.
Sei also $b \neq 0$. Angenommen unsere Behauptung wäre falsch und es gälte $a^2 - 2b^2 = 0$. Dann aber folgt:

$$a^2 = 2b^2 \Rightarrow \left(\frac{a}{b}\right)^2 = 2 \Rightarrow \frac{a}{b} = \sqrt{2} \Rightarrow \sqrt{2} \in \mathbb{Q}$$

Und das ist ein Widerspruch, denn bekanntlich gilt $\sqrt{2} \notin \mathbb{Q}$. Sei also nun $a + b\sqrt{2} \in U$ mit $a + b\sqrt{2} \neq 0$ beliebig. Gesucht ist nun ein Element $c + d\sqrt{2} \in U$ mit $(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = 1$.
Definiere $c := \frac{a}{a^2 - 2b^2}$ und $d := -\frac{b}{a^2 - 2b^2}$. Nach obiger Behauptung sind diese Ausdrücke definiert. Dann folgt:

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (a + b\sqrt{2}) \cdot \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a^2 - 2b^2}{a^2 - 2b^2} = 1$$

Offensichtlich gilt $c, d \in \mathbb{Q}$ und damit liegt das Inverse bzgl. $\cdot$ zu einem Element aus $U \backslash \{0\}$ wieder in U und daraus folgt, dass U ein Körper ist. Und das war zu zeigen. □

Aufgabe 3

Vorausgesetzt sei die Division mit Rest: Zu $a \in \mathbb{Z}, b \in \mathbb{N}$ gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit $0 \leq r < b$ und $a = qb + r$.

(a) Seien $n, m \in G$ beliebig. Wende die Division mit Rest auf $a := n \cdot m$ und $b := p$ an und erhalte Zahlen $q, r \in \mathbb{Z}$ mit $0 \leq r < p$ und $nm = qp + r$. Damit ist aber $nm - r = qp$. Zunächst gilt $r > 0$, denn falls $r = 0$, so folgt $nm = qp$, also ist p ein Teiler von nm und da p eine Primzahl ist also ein Teiler von n oder von m, was aber nicht möglich ist, da sowohl $n < p$ als auch $m < p$ gilt. Also ist $r \in \mathbb{N}$.
Behauptung: $n * m = r$. Dazu genügt es zu zeigen, dass r die kleinste natürliche Zahl ist, für die $nm - r$ ein ganzzahliges Vielfaches von p ist. Angenommen es gibt ein $0 < k \leq r$ mit $nm - k = q'p$. Dann folgt:

$$r - k = (nm - qp) - (nm - q'p) = (q' - q)p$$

Es gilt aber $0 \leq r-k < p$, also kann $r-k$ nur dann ganzzahliges Vielfaches von p sein, wenn gilt $r-k=0$ also $r=k$. Damit folgt $n*m=r$ und $1 \leq r \leq p-1$, also $n*m \in G$, was zu zeigen war.

(b) Wieder ist die Definition der Verknüpfung symmetrisch in n und m, also ist die Verknüpfung in jedem Fall kommutativ. Weisen wir wieder die Eigenschaften nach:

(i) **Assoziativität**
Seien $a, b, c \in G$. Dann gilt $a*b = ab - qp$ für ein $q \in \mathbb{Z}$. Ebenso gilt $(a*b)*c = (a*b)c - q'p$ für ein $q' \in \mathbb{Z}$. Es folgt:

$$(a*b)*c = (ab-qp)*c = (ab-qp)c - q'p = abc - (qc+q')p$$

Damit ist $(a*b)*c$ der eindeutig bestimmte Rest, der bei Division von abc durch p bleibt.
Analog gibt es ganze Zahlen $s, s' \in \mathbb{Z}$ mit $b*c = bc-sp$ und $a*(b*c) = a(b*c) - s'p$. Zusammen ergibt sich wieder:

$$a*(b*c) = a*(bc-sp) = a(bc-sp) - s'p = abc - (as+s')p$$

Also ist auch $a*(b*c)$ der eindeutig bestimmte Rest, der bei Division von abc durch p bleibt. Damit folgt $(a*b)*c = a*(b*c)$ und das war zu zeigen.

(ii) **Neutrales Element**
Sei $a \in G$ beliebig. Behauptung: für $1 \in G$ gilt $1*a = a*1 = a$.
Nach Definition ist $a*1$ die kleinste natürliche Zahl, für die $a - a*1$ ein Vielfaches von p ist. Da $a < p$ folgt sofort: $a*1 = a$.

(iii) **Inverses Element**
Zu $a \in G$ betrachte die Menge $M := \{a*x : x \in G\} \subseteq G$. Seien $x, y \in G$ mit $a*x = a*y$. Behauptung: dann gilt $x = y$. Wäre dies der Fall, so würde folgen, dass M genau $p-1$ Elemente haben muss, also gleich G sein muss. Dann aber gilt $1 \in M$ und es gibt ein inverses Element zu a.
Beweis der Behauptung: Seien also $x, y \in G$ mit $a*x = a*y$. Ohne Beschränkung der Allgemeinheit darf man annehmen, dass gilt $x \geq y$. Dann gibt es wie oben ganze Zahlen $q, q' \in \mathbb{Z}$ mit $a*x = ax - qp$ und $a*y = ay - q'p$. Daraus folgt:

$$ax - qp = ay - q'p \Rightarrow a(x-y) = (q-q')p$$

Also teilt p das Produkt $a(x-y)$. Da $a < p$ ist p aber kein Teiler von a. Da p eine Primzahl ist, folgt also automatisch, dass p die Differenz $x-y$ teilt. Es gilt aber $0 \leq x-y < p$ und damit ist $x-y=0$ bzw. $x=y$, womit auch die Behauptung bewiesen wäre.

All dies zeigt die Aufgabe. □