7. **Abstract Algebra** – a study of the structure of number systems with a binary operation.

① **Group** – is a collection of objects G (elements), together with a binary operation, $*$, that obey the following rules:

- **Closure** – If $a, b \in G$, then $a * b \in G$.
- **Associative** – If $a, b, c \in G$, then $(a * b) * c = a * (b * c)$

- **Identity** – $\exists\, e \in G \ni: a * e = e * a = a$ for all $a \in G$.
- **Inverse** – If $a \in G$, $\exists\, b \in G \ni: a * b = b * a = e$.

Ex: $G = \mathbb{Z}$, $* = +$, $e = 0$, Inverses are negatives

Non-Ex: $G = \mathbb{R} \setminus \mathbb{Q} \cup \{0\} = \mathbb{I} \cup \{0\}$, $* = +$, $e = 0$, Fails Closure

$a = 1 + \sqrt{2}$

$b = -\sqrt{2}$

$a + b = 1 \notin G$

Ex: $G = \mathbb{Q}^+$, $* = \cdot$, $e = 1$, Inverses are Reciprocals

Ex: $G =$ set of all 2×2 matrices w/ det $\neq 0$, $*$ = matrix multiplication, $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, Inverses

Ex: $\mathbb{Z}_{31} = \{0, 1, 2, \ldots, 30\}$

$* = +$ mod 31 (e.g. $23 + 14 = 37 \bmod 31 = 6$)

② **Field** – a collection of objects that forms a group under two different binary operations, $\oplus$ and $\odot$, which are compatible by a distributive law:

$$a \odot (b \oplus c) = a \odot b + a \odot c$$

Ex: $F = \mathbb{R}$, $+, \cdot$, $e_+ = 0$, $e_\cdot = 1$

Ex: $F = \mathbb{Q}$, $+, \cdot$, $e_+ = 0$, $e_\cdot = 1$

Ex: $F = \mathbb{Z}_{31}$

$+ \bmod 31$, $\cdot \bmod 31$

$e_+ = 0$, $e_\cdot = 1$

③ **Completeness** – a field is complete iff every polynomial with coefficients in the field has all of its roots in the field.

Ex: Is $\mathbb{Q}$ complete? No.

$p = 1x^2 + 0x - 2 = 0$

$x = \pm\sqrt{2} \notin \mathbb{Q}$.

Ex: Is $\mathbb{R}$ complete? No

$p = 1x^2 + 0x - 1 = 0$

$x = \pm\sqrt{-1} = \pm i \notin \mathbb{R}$

Ex: Is $\mathbb{C}$ complete? Yes.

FTA

$\mathbb{C}$ are the smallest complete field that contains $\mathbb{Z}$.

④ **Extension Field** – if a field is not complete and $q \notin F$, what is the smallest field containing q?

$F(q)$ = (smallest) extension field of F containing q.

$F(q) = \{ a + b \cdot q \mid a, b \in F \}$

Ex: $\frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2} = 0 + \frac{1}{2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$

$7 + 3\sqrt{2}$ and want mult. inverse, then

$$\frac{1}{7+3\sqrt{2}} \cdot \frac{7-3\sqrt{2}}{7-3\sqrt{2}} = \frac{7-3\sqrt{2}}{49-18} = \frac{7}{31} - \frac{3}{31}\sqrt{2}$$

Ex: $\mathbb{R}(\sqrt{-1}) = \mathbb{R}(i) = \{ a + bi \mid a, b \in \mathbb{R} \} = \mathbb{C}$

$3 + 2i \in \mathbb{C}$ and we need mult. inverse, then

$$\frac{1}{3+2i} \cdot \frac{3-2i}{3-2i} = \frac{3-2i}{9-4i^2} = \frac{3-2i}{13} = \frac{3}{13} - \frac{2}{13}i$$

⑤ **Algebraic Number** – a number that is a root of a polynomial w/ integer (or $\mathbb{Q}$) coefficients.

Ex: $\sqrt[3]{5}$ is root of $1x^3 - 5 = 0$

$\frac{2}{7}$ is root of $7x - 2 = 0$

$\sqrt{3 + \sqrt{7}} = x$

$3 + \sqrt{7} = x^2$

$$(\sqrt{7})^2 = (x^2 - 3)^2$$

$$7 = x^4 - 6x^2 + 9$$

$$0 = 1x^4 - 6x^2 + 2$$

Transcendental Numbers are all other numbers, e.g. e, π