Dictionary

Prajwal Neupane

1 Dictionary

1. **Automorphism**:
   - Maps structure to itself
   - preserves operations of structure
   - is a bijection
   - think of the concept of all permutations being all bijections from a set to itself.
   - Def: A field automorphism $\sigma : K \to K$ satisfies:
     - $\sigma(a + b) = \sigma(a) + \sigma(b)$
     - $\sigma(ab) = \sigma(a)\sigma(b)$
     - $\sigma(1) = 1$
   - set of all automorphisms of a field K is denoted Aut(K).
   - we can fix a sub-field, $F \subsetneq K$, look at $Aut(K/F)$: automorphisms of K that fix every element of F.
   - Example:
     - $Aut(\mathbb{Q}) = \{id\}$
     - $Aut(\mathbb{R}) = \{id\}$
     - $Aut(\mathbb{C}/\mathbb{R}) = \{id, conjugate\}$
2. **Group:**
   - A set G with a binary operation $*$: $G \times G \to G$ satisfying:
     - Closure: $\forall a, b \in G,\ a * b \in G$
     - Associativity: $(a * b) * c = a * (b * c)$
     - Identity: $\exists e \in G$ such that $a * e = e * a = a$
     - Inverse: $\forall a \in G,\ \exists a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$
   - Notation: $(G, *)$ or just G
   - If $a * b = b * a\ \forall a, b \in G$, then G is called **abelian**.
   - Examples:
     - $(\mathbb{Z}, +)$: additive group of integers
     - S_n: symmetric group on n elements (non-abelian for $n \geq 3$ why? $\to$ can always find elements that don't commute.)

- $GL_n(\mathbb{R})$: invertible $n \times n$ real matrices under multiplication (abelian? no because generally for $n \geq 2$ matrix multiplication is not commutative.)

3. **Field**:
   - set with two operations, add and multiply, such that:
     - $(F, +)$ is an abelian group with identity 0
     - nonzero elements form an abelian group (zero does not have multiplicative inverse, $(F \setminus \{0\}, \cdot)$ is an abelian group with identity 1
     - distributive law holds $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$
     - Examples: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$

4. **Splitting field**:
   - let $f(x) \in F[x]$ be a polynomial over a field F (say $F = \mathbb{Q}$)
   - The splitting field of f over F is the smallest extension $K \supsetneq F$ such that:
     - f(x) factors into linear factors in K[x].
     - K is generated by roots of f.
     - K is the smallest field where this happens
   - "The smallest field that contains all roots of f(x) and "nothing extra.""
   - Ex: $f(x) = x^2 - 2 \in \mathbb{Q}[x]$
     - doesn't factor in $\mathbb{Q}$, roots are $\pm\sqrt{2}$
     - splitting field is $\mathbb{Q}(\sqrt{2})$