Algebra Definitions

Peter Kagey

May 2019

1 Groups

1.1 Notation and definitions

1.1.1 Basic definitions

Definition 1.1.1.1 (Normal subgroup)**.** Let G be a group and K be a subgroup of G. If $gkg^{-1} \in K$ for all $k \in K$ and $g \in G$, then K is called a normal subgroup of G and is denoted $K \trianglelefteq G$.

Definition 1.1.1.2 (Simple group)**.** A group G is called a simple group is a group whose only normal subgroups are $\{e\}$ and G.

Definition 1.1.1.3 (Semidirect product)**.** Let $K \trianglelefteq G$ and $Q \leq G$. A group G is a semidirect product of K by Q (denoted $G = K \ltimes Q$) if there exists $Q_1 \cong Q$ such that Q_1 is a complement of K in G, that is $K \cap Q_1 = 1$ and $KQ_1 = G$.

1.1.2 Galois Theory

Definition 1.1.2.1 (Normal series)**.** A normal series of a group G is a sequence of subgroups

$$G = G_0 \geq G_1 \geq \ldots \geq G_n = 1$$

in which $G_{i+1} \trianglelefteq G_i$ for all i.

Definition 1.1.2.2 (Factor groups)**.** The factor groups of a normal series are the groups G_i/G_{i+1} for $i = 0, 1, \ldots, n-1$.

Definition 1.1.2.3 (Length)**.** The length of a a normal series is the number of nontrivial factor groups.

Definition 1.1.2.4 (Solvable group)**.** A finite group is solvable if it has a normal series whose factor groups are cyclic of prime order.

1.1.3 Centralizer/Normalizer

Definition 1.1.3.1 (Center)**.** The center of a group G, denoted by $Z(G)$, is the set of all $a \in G$ that commute with every element of G.

Definition 1.1.3.2 (Centralizer)**.** The centralizer of a subset S of a group G is defined to be

$$C_G(S) = \{g \in G \mid gs = sg \text{ for all } s \in S\}.$$

Definition 1.1.3.3 (Normalizer)**.** The centralizer of a subset S in the group G is defined to be

$$N_G(S) = \{g \in G \mid gS = Sg\}.$$

Definition 1.1.3.4 (Commutator)**.** If $a, b \in G$, the commutator of a and b, denoted $[a, b]$, is

$$[a, b] = aba^{-1}b^{-1},$$

and the commutator subgroup of G, denoted G', is the subgroup of G generated by all of the commutators.

Definition 1.1.3.5 (Class equation)**.** Partition G into its conjugacy classes, with x_i the representative of the ith conjugacy class. The class equation of the finite group G is

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)].$$

1.1.4 Group Actions

Definition 1.1.4.1 (Group action)**.** Let G be a group and X be a set. Then a group action on X is a function $\varphi \colon G \times X \to X$ denoted $\varphi(g, x) = g \cdot x$ and satisfying

(i) Identity: group action by the identity is trivial for all $x \in X$: $1 \cdot x = x$.

(ii) Compatibility: $(gh) \cdot x = g \cdot (h \cdot x)$.

And X is called a G-set.

Definition 1.1.4.2 (Orbit)**.** The orbit of an element $x \in X$ is denoted by

$$G \cdot x = \{g \cdot x \mid g \in G\}$$

Definition 1.1.4.3 (Stabilizer subgroup)**.** The stabilizer subgroup of G with respect to $x \in X$ is denoted

$$G_x = \{g \in G \mid g \cdot x = x\}$$

Definition 1.1.4.4 (Transitive)**.** A group action is called transitive is for each $x, y \in X$ there exists some $g \in G$ such that $g \cdot x = y$.

1.2 Theorems

Theorem 1.2.1 (First isomorphism theorem)**.** If $\varphi\colon G \to H$ is a group homomorphism then $\ker(\varphi) \trianglelefteq G$ and $G/\ker(\varphi) \cong \varphi(G)$.

Theorem 1.2.2 (Second isomorphism theorem)**.** Let G be a group with $S \leq G$ and $N \trianglelefteq G$. Then

1. $SN \leq G$
2. $S \cap N \trianglelefteq S$, and
3. $(SN)/N \cong S/(S \cap N)$.

Strictly speaking, N does not have to be a normal subgroup as long as S is a subgroup of the normalizer of N, $S \leq N_G(N)$.

Theorem 1.2.3 (Third isomorphism theorem)**.** Let G be a group with normal subgroup $N \trianglelefteq G$. Then

1. If $K \leq G$ (resp. $K \trianglelefteq G$) such that $N \subseteq K \subseteq G$, then $K/N \leq G/N$ (resp. $K/N \trianglelefteq G/N$).
2. Every subgroup (resp. normal subgroup) of G/N is of the form K/N, for some subgroup (resp. normal subgroup) $K \subset G$ such that $N \subseteq K \subseteq G$.
3. If $K \trianglelefteq G$ such that $N \subseteq K \subseteq G$, then $(G/N)/(K/N) \cong G/K$.

Theorem 1.2.4 (Simplicity of the A_n)**.** A_n is simple for all $n \geq 5$.

Theorem 1.2.5 (Sylow's theorem)**.**

(i) If P is a Sylow p-subgroup of a finite group G, then all Sylow p-subgroups of G are conjugate to P.

(ii) If there are r Sylow p-subgroups, then r divides $|G|$ and $r \equiv 1 \bmod p$.

Theorem 1.2.6 (Fundamental Theorem of Abelian Groups)**.** If G and H are finite abelian groups, then $G \cong H$ if and only if, for all primes p, they have the same elementary divisors.

Theorem 1.2.7. Let G be a finite group and p be the least prime divisor of $|G|$. Then if H is a subgroup of G such that $[G : H] = p$, then $H \trianglelefteq G$.

2 Fields

2.1 Notation and definitions

2.1.1 Basic definitions

Definition 2.1.1.1 (Degree of a field extension)**.** Suppose that E/k is a field extension. Then E may be considered as a vector space over k. The dimension of this vector space is called the degree of the field extension and is denoted by $[E : k]$.

Definition 2.1.1.2 (Field automorphism)**.** A field automorphism of a field K is an isomorphism $\phi\colon K \to K$. In particular,

$$\phi(a + b) = \phi(a) + \phi(b) \text{ and}$$
$$\phi(ab) = \phi(a)\phi(b).$$

Definition 2.1.1.3 (Splitting field)**.** A splitting field of a polynomial p over a field K is a field extension $L \supseteq K$ over which p factors into linear factors.

Definition 2.1.1.4 (Separable polynomial)**.** A polynomial p is called separable if if factors into distinct linear factors in its splitting field.

Definition 2.1.1.5 (Separable extension)**.** A separable extension is an field extension $E \supseteq F$ such that for every $\alpha \in E$, the minimal polynomial of α over F is a separable polynomial.

Definition 2.1.1.6 (Normal extension)**.** A normal extension $K \supseteq L$ is one for which every polynomial that is irreducible over K either has no root in L or splits into linear factors in L.

Definition 2.1.1.7 (Galois extension)**.** A Galois extension is an algebraic field extension E/F that is normal and separable.

Definition 2.1.1.8 (Galois group)**.** Let $E \supseteq F$ be a field extension. The Galois group $\mathrm{Gal}(E/F)$ is the set of automorphisms of E that fix F under function composition.

Definition 2.1.1.9 (Galois correspondence)**.** Let $E \supseteq F$ be a finite, Galois extension. The Galois correspondence is the bijection between intermediate fields $F \supseteq K \supset E$ and subgroups of the Galois group E/F.

Definition 2.1.1.10 (Trace)**.** ???

Definition 2.1.1.11 (Norm)**.** ???

Definition 2.1.1.12 (Radical extension)**.** A radical extension of a field K is an extension that is obtained by adjoining a sequence of nth roots of elements of K.

Definition 2.1.1.13 (Finite field)**.** A finite field is a field with a finite number of elements. Note: any finite field has p^k elements for some prime p and $k \in \mathbb{N}$.

Definition 2.1.1.14 (Cyclotomic extension)**.** A cyclotomic extension $\mathbb{Q}(\xi_n)$ of $\mathbb{Q}$ is an extension formed by adjoining a primitive nth root of unity.

Definition 2.1.1.15 (Algebraic closure)**.** An algebraic closure of a field K is an algebraic extension F/K such that F contains a root for every non-constant polynomial in $F[x]$.

2.2 Theorems

Theorem 2.2.1 (Isomorphism extension theorem)**.** Let F be a field and $\phi\colon F \to F'$ an isomorphism. Then if E is an extension field of F, ϕ can be extended into an isomorphism $\tau\colon E \to E'$.

Theorem 2.2.2 (Fundamental theorem of Galois theory)**.** Let E/k be a finite Galois extension with Galois group $G = \mathrm{Gal}(E/k)$. The function

$$\gamma\colon \mathrm{Sub}(\mathrm{Gal}(E/k)) \to \mathrm{Int}(E/k),$$

defined by $H \mapsto E^H$, is an order reversing bijection whose inverse maps $B \mapsto \mathrm{Gal}(E/B)$.

Theorem 2.2.3 (Primitive element theorem)**.** Finite separable extensions are simple.