Algebra Theorems

http://mathtuition88.com

July 27, 2016

Contents

1 Linear Algebra

2 Group Theory

2.1 First Isomorphism Theorem

Let G and H be groups, and let $\phi : G \to H$ be a homomorphism. Then $\phi(G) \cong G/\ker\phi$.

2.2 Second Isomorphism Theorem

Let G be a group. Let $S \leq G$ and $N \trianglelefteq G$. Then $(SN)/N \cong S/(S \cap N)$.

2.3 Third Isomorphism Theorem

Let G be a group, and $N \trianglelefteq G$, $K \trianglelefteq G$ such that $N \subseteq K \subseteq G$. Then $(G/N)/(K/N) \cong G/K$.

2.4 Correspondence Theorem

Let $N \trianglelefteq G$. There exists a bijection $\phi : \{\text{all subgroups } H \text{ such that } N \subseteq H \subseteq G\} \to \{\text{subgroups of } G/N\}$, with $\phi(H) = H/N$.

2.5 Fundamental Theorem of Finitely Generated Abelian Groups

2.5.1 Primary decomposition

Every finitely generated abelian group G is isomorphic to a group of the form

$$\mathbb{Z}^n \oplus \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_t}$$

where $n \geq 0$ and $q_1, \ldots, q_t$ are powers of (not necessarily distinct) prime numbers. The values of $n, q_1, \ldots, q_t$ are (up to rearrangement) uniquely determined by G.

2.5.2 Invariant factor decomposition

We can also write G as a direct sum of the form

$$\mathbb{Z}^n \oplus \mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_u},$$

where $k_1 \mid k_2 \mid k_3 \mid \cdots \mid k_u$. Again the rank n and the invariant factors $k_1, \ldots, k_u$ are uniquely determined by G.

2.6 Sylow Theorems

Let G be a finite group.

2.6.1 Theorem 1

For every prime factor p with multiplicity n of the order of G, there exists a Sylow p-subgroup of G, of order p^n.

2.6.2 Theorem 2

All Sylow p-subgroups of G are conjugate to each other, i.e. if H and K are Sylow p-subgroups of G, then there exists an element $g \in G$ with $g^{-1}Hg = K$.

2.6.3 Theorem 3

Let p be a prime such that $|G| = p^n m$, where $p \nmid m$. Let n_p be the number of Sylow p-subgroups of G. Then:

- $n_p \mid m$, which is the index of the Sylow p-subgroup in G.
- $n_p \equiv 1 \pmod{p}$.

2.6.4 Theorem 3b (Proof)

We have $n_p = [G : N_G(P)]$, where P is any Sylow p-subgroup of G and N_G denotes the normalizer.

Proof. Let P be a Sylow p-subgroup of G and let G act on $\mathrm{Syl}_p(G)$ by conjugation. We have $|\mathrm{Orb}(P)| = n_p$, $\mathrm{Stab}(P) = \{g \in G : gPg^{-1} = P\} = N_G(P)$.

By the Orbit-Stabilizer Theorem, $|\mathrm{Orb}(P)| = [G : \mathrm{Stab}(P)]$, thus $n_p = [G : N_G(P)]$. □

2.7 Orbit-Stabilizer Theorem (Proof)

Let G be a group which acts on a finite set X. Then

$$|\mathrm{Orb}(x)| = [G : \mathrm{Stab}(x)] = \frac{|G|}{|\mathrm{Stab}(x)|}.$$

Proof. Define $\phi : G/\text{Stab}(x) \to \text{Orb}(x)$ by

$$\phi(g\text{Stab}(x)) = g \cdot x.$$

Well-defined:

Note that $\text{Stab}(x)$ is a subgroup of G. If $g\text{Stab}(x) = h\text{Stab}(x)$, then $g^{-1}h \in \text{Stab}(x)$. Thus $g^{-1}hx = x$, which implies $hx = gx$, thus ϕ is well-defined.

Surjective:

ϕ is clearly surjective.

Injective:

If $\phi(g\text{Stab}(x)) = \phi(h\text{Stab}(x))$, then $gx = hx$. Thus $g^{-1}hx = x$, so $g^{-1}h \in \text{Stab}(x)$. Thus $g\text{Stab}(x) = h\text{Stab}(x)$.

By Lagrange's Theorem,

$$\frac{|G|}{|\text{Stab}(x)|} = |G/\text{Stab}(x)| = |\text{Orb}(x)|.$$

□

2.8 Semidirect Product

2.8.1 Outer Semidirect Product

Given any two groups N and H and a group homomorphism $\phi : H \to \text{Aut}(N)$, we can construct a new group $N \rtimes_\phi H$, called the (outer) semidirect product of N and H with respect to ϕ, defined as follows.

(i) The underlying set is the Cartesian product $N \times H$.

(ii) The operation, $\bullet$, is determined by the homomorphism ϕ:

$\bullet : (N \rtimes_\phi H) \times (N \rtimes_\phi H) \to N \rtimes_\phi H$

$(n_1, h_1) \cdot (n_2, h_2) = (n_1\phi_{h_1}(n_2), h_1h_2)$

for $n_1, n_2 \in N$ and $h_1, h_2 \in H$.

This defines a group in which the identity element is (e_N, e_H) and the inverse of the element (n, h) is $(\phi_{h^{-1}}(n^{-1}), h^{-1})$.

Pairs (n, e_H) form a normal subgroup isomorphic to N, while pairs (e_N, h) form a subgroup isomorphic to H.

2.9 Inner Semidirect Product (Definition)

Given a group G with identity element e, a subgroup H, and a normal subgroup $N \lhd G$; then the following statements are equivalent:

- G is the product of subgroups, $G = NH$, where the subgroups have trivial intersection, $N \cap H = \{e\}$.
- For every $g \in G$, there are unique $n \in N$ and $h \in H$, such that $g = nh$.

If these statements hold, we define G to be the semidirect product of N and H, written $G = N \rtimes H$.

2.10 Inner Semidirect Product Implies Outer Semidirect Product

Suppose we have a group G with $N \lhd G$, $H \leq G$ and every element $g \in G$ can be written uniquely as $g = nh$ where $n \in N$, $h \in H$.

Define $\phi : H \to \mathrm{Aut}(N)$ as the homomorphism given by $\phi(h) = \phi_h$, where $\phi_h(n) = hnh^{-1}$ for all $n \in N$, $h \in H$.

Then G is isomorphic to the semidirect product $N \rtimes_\phi H$, and applying the isomorphism to the product, nh, gives the tuple, (n, h). In G, we have

$$(n_1 h_1)(n_2 h_2) = n_1 h_1 n_2 (h_1^{-1} h_1) h_2 = (n_1 \phi_{h_1}(n_2))(h_1 h_2) = (n_1, h_1) \cdot (n_2, h_2)$$

which shows that the above map is indeed an isomorphism.

2.11 Necessary and Sufficient Conditions for Semidirect Product to be Abelian (Proof)

The semidirect product $N \rtimes_\varphi H$ is abelian iff N, H are both abelian and $\varphi : H \to \mathrm{Aut}(N)$ is trivial.

Proof. $(\implies)$

Assume $N \rtimes_\varphi H$ is abelian. Then for any $n_1, n_2 \in N$, $h_1, h_2 \in H$, we have

$$(n_1, h_1) \cdot (n_2, h_2) = (n_2, h_2) \cdot (n_1, h_1)$$
$$(n_1\varphi_{h_1}(n_2), h_1h_2) = (n_2\varphi_{h_2}(n_1), h_2h_1).$$

This implies $h_1h_2 = h_2h_1$, thus H is abelian.

Consider the case $n_1 = n_1 = n$. Then for any $n \in N$, $n\varphi_{h_1}(n) = n\varphi_{h_2}(n)$. Multiplying by n^{-1} on the left gives $\varphi_{h_1}(n) = \varphi_{h_2}(n)$ for any $h_1, h_2 \in H$. Thus $\varphi_h(n) = \varphi_{e_H}(n) = n$ for all $h \in H$ so φ is trivial.

Consider the case where $h_1 = h_2 = e_H$. Then we have $n_1n_2 = n_2n_1$, so N has to be abelian.

$(\impliedby)$

This direction is clear. $\square$

3 Ring/Module Theory

3.1 Balanced product

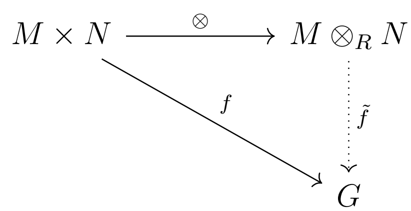
For a ring R, a right R-module M, a left R-module N, and an abelian group G, a map $\phi : M \times N \to G$ is said to be R-balanced, if for all $m, m' \in M$, $n, n' \in N$, and $r \in R$ the following hold:

$$\phi(m, n + n') = \phi(m, n) + \phi(m, n')$$
$$\phi(m + m', n) = \phi(m, n) + \phi(m', n)$$
$$\phi(m \cdot r, n) = \phi(m, r \cdot n)$$

3.2 Tensor Product

For a ring R, a right R-module M, a left R-module N, the tensor product over R, $M \otimes_R N$, is an abelian group together with a balanced product $\otimes : M \times N \to M \otimes_R N$ which is universal:

For every abelian group G and every balanced product $f : M \times N \to G$, there is a unique group homomorphism $\tilde{f} : M \otimes_R N \to G$ such that $\tilde{f} \circ \otimes = f$.



3.3 Eisenstein's Criterion

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $\mathbb{Z}[x]$. If there exists a prime p such that:

(i) $p \mid a_i$ for $i \neq n$,

(ii) $p \nmid a_n$, and

(iii) $p^2 \nmid a_0$

then f is irreducible over $\mathbb{Q}$.

4 Galois/Field Theory

4.1 Finite extension is Algebraic extension (Proof)

Let L/K be a finite field extension. Then L/K is an algebraic extension.

Proof. Let L/K be a finite extension, where $[L : K] = n$. Let $\alpha \in L$. Consider $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ which has to be linearly dependent over K since there are $n+1$ elements. Thus, there exists $c_i \in K$ (not all zero) such that $\sum_{i=0}^{n} c_i \alpha^i = 0$, so α is algebraic over K. □

4.2 Finitely Generated Algebraic Extension is Finite (Proof)

Let L/K be a finitely generated algebraic extension. Then L/K is a finite extension.

Proof. Since L/K is finitely generated, $L = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in K$. Since L/K is algebraic, each α_i is algebraic over K. Denote $L_i := K(\alpha_1, \ldots, \alpha_i)$ for $1 \leq i \leq n$. Then $L_i = L_{i-1}(\alpha_i)$ for each i. Since α_i is algebraic over K, it is also algebraic over L_{i-1}, so there exists a polynomial g_i with coefficients in L_{i-1} such that $g_i(\alpha_i) = 0$. Thus $[L_i : L_{i-1}] \leq \deg g_i < \infty$. Similarly $[L_1 : K] < \infty$. By Tower Law, $[L : K] = [L_n : L_{n-1}][L_{n-1} : L_{n-2}] \ldots [L_1 : K] < \infty$. □

4.3 Separable Polynomial

A polynomial over F is said to be separable if it has no multiple roots (i.e., all its roots are distinct).

4.4 Galois Group of Polynomial

Let $f(x)$ be a separable polynomial over F. Let K be the splitting field over F of $f(x)$. Then the Galois group of $f(x)$ over F is defined to be $\mathrm{Gal}(K/F)$.