Modern Algebra 1 — Theorem List 1

Spring 2010

Throughout what follows, G is a group, $a_i \in G$, e denotes the identity in G (when multiple groups are involved the identity in question is understood), and m, n denote arbitrary integers. S_n will denote the symmetric group on n letters. It should also be understood that this list of facts is not meant to be a comprehensive group (no pun intended) of things to know for the upcoming midterm.

Theorem 1. *Let G be a group.*

a. *The identity element in G is unique.*

b. *The inverse of $a \in G$ is unique.*

c. *Given $a_1, a_2, \ldots, a_n \in G$, the product $a_1 a_2 \cdots a_n$ is independent of how the elements in the product are pairwise associated.*

Theorem 2. *Given $a \in G$ and $m, n \in \mathbb{Z}$, the usual rules of exponents hold. That is:*

a. $(a^m)(a^n) = a^{m+n}$;

b. $(a^m)^n = a^{mn}$;

a. $a^0 = e$.

Theorem 3. *If $\sigma \in S_n$ is an m-cycle then $\sigma^k = (1)$ if and only if m divides k.*

Theorem 4. *If $\sigma \in S_n$ then $|\sigma|$ is the least common multiple of the the lengths of the cycles in the cycle decomposition of σ.*

Theorem 5. *The group D_n is generated by two elements r and f which satisfy $r^n = f^2 = e$ and $rf = fr^{-1} = fr^{n-1}$, so that $D_n = \langle r, f \rangle = \{f^i r^j \mid i = 0, 1\, j = 0, 1, \ldots, n-1\}$, and each element specified is distinct.*

Theorem 6. *If G is finite then every element of G has finite order.*

Theorem 7. *Let $a \in G$. Then $a^n = e$ if and only if the order of a divides n.*

Theorem 8. *Let $a \in G$. Then*

$$|a^n| = \frac{|a|}{\gcd(|a|, n)}.$$

Theorem 9. *If $m \in Z_n$ then*

$$|m| = \frac{n}{\gcd(m, n)}.$$

Theorem 10. *A nonempty subset H of G is a subgroup if and only if the following two conditions hold.*

a. *For all $a, b \in H$, $ab \in H$.*

b. *For all $a \in H$, $a^{-1} \in H$.*

Theorem 11. *A nonempty subset H of G is a subgroup if and only if for all $a, b \in H$, $ab^{-1} \in H$.*

Theorem 12. *Every subgroup H of $\mathbb{Z}$ is of the form $H = \langle n \rangle = \{kn \mid k \in \mathbb{Z}\}$. If $H \neq \{0\}$ then n may be taken to be the least positive element of H, and n uniquely determines H.*

Theorem 13. *Let $f : G \to H$ be a group homomorphism. Then:*

a. $f(e) = e$;

b. $f(a^{-1}) = f(a)^{-1}$ *for all* $a \in G$;

c. $f(a^n) = f(a)^n$ *for all* $a \in G$ *and* $n \in \mathbb{Z}$;

d. *If* $K \leq G$ *then* $f(K) \leq H$;

e. *If* $K \leq H$ *then* $f^{-1}(K) \leq G$.

Theorem 14. *The composition of group homomorphisms is a homomorphism.*

Theorem 15. *The composition of group isomorphisms is an isomorphism. The inverse of a group isomorphism is an isomorphism.*

Theorem 16. *A group homomorphism is injective if and only if its kernel is trivial.*

Theorem 17. *If $f : G \to H$ is an injective homomorphism then $G \cong \operatorname{Im} f$.*

Theorem 18. *Let $a \in G$. Conjugation by a ($c_a(x) = axa^{-1}$) is an automorphism of G (called an inner automorphism of G). The map $a \mapsto c_a$ is a homomorphism of G to $\operatorname{Aut} G$. Its kernel is $Z(G)$.*