

Math 113 Theorems.

1. **Prop.** The relation  $\equiv \pmod{n}$  is an equivalence relation.
2. **Prop.**  $\mathbb{Z}/n\mathbb{Z}$  has exactly  $n$  elements.
  - (a) **Prop 0.** If  $i \in [j]$ , then  $j \in [i]$  (in  $\mathbb{Z}/n\mathbb{Z}$ ).
  - (b) **Prop 1.** If  $[i] \cap [j] \neq \emptyset$ , then  $[i] = [j]$ .
  - (c) **Prop 2.** If  $i \neq j$  and  $0 \leq i, j \leq n-1$ , then  $[i] \cup [j] = \emptyset$ .
  - (d) **Prop 3.** Every  $x \in \mathbb{Z}$  belongs to one of  $[0], \dots, [n-1]$ .
3. **Prop.** Addition is correctly (well-defined) defined on  $\mathbb{Z}/n\mathbb{Z}$  by  $[a] + [b] = [a+b]$ .
4. **Prop 3.17.** The identity element in any group is unique.
5. **Prop 3.18.** The inverse is unique for any element  $g$  in a group  $G$ .
6. **Prop 3.19.** For any  $a, b \in G$ , where  $G$  is a group,  $(a \star b)^{-1} = b^{-1}a^{-1}$ .
7. **Prop 3.20.** For any  $g \in G$ , where  $G$  is a group, then  $(g^{-1})^{-1} = g$ .
8. **Theorem 5.1.**  $S_n$  is a group with  $n!$  elements where the binary operation is the composition of maps.
9. **Prop 5.8.** Let  $\sigma$  and  $\tau$  be two disjoint cycles in  $S_X$ . Then,  $\sigma\tau = \tau\sigma$ .
10. **Theorem 5.9.** Every permutation in  $S_n$  can be written as the product of disjoint cycles.
11. **Prop 5.12.** Any permutation of a finite set containing at least 2 elements can be written as the product of transpositions.
12. **Lemma 5.14.** If the identity is written as the product of  $r$  transpositions,  $\text{id} = \tau_1 \dots \tau_r$ , then  $r$  is even.
13. **Theorem 5.15.** If a permutation  $\sigma$  can be expressed as the product of an even number of transpositions, then any other product of transpositions equaling  $\sigma$  must also contain an even number of transpositions. Similarly, in the case of when  $\sigma$  is odd.
14. **Prop 3.30.** A subset  $H$  of  $G$  is a subgroup iff:

- (a)  $e \in G$  also satisfies  $e \in H$ .
  - (b) If  $h_1, h_2 \in H$ , then  $h_1 h_2 \in H$ .
  - (c) If  $h \in H$ , then  $h^{-1} \in H$ .
15. **Prop 3.31.** Let  $H$  be a subset of a group  $G$ . Then,  $H$  is a subgroup of  $G$  iff  $H \neq \emptyset$  and if  $g, h \in H$ , then  $gh^{-1} \in H$ .
16. **Theorem 4.3.** Take a group  $G$  and an element  $a \in G$ . Consider a cyclic subgroup  $\langle a \rangle$ . Then,  $\langle a \rangle$  is a minimal subgroup of  $G$  such that  $a$  is in it (minimality: if  $H$  is a subgroup of  $G$  and  $a \in H$ , then  $\langle a \rangle$  is a subgroup of  $H$ ).
17. **Theorem 4.9.** Every cyclic group is abelian.
18. **Prop 11.4.** Let  $\phi : G \rightarrow H$  be a homomorphism. Then:
- (a)  $\phi(e_G) = e_H$ .
  - (b)  $\phi(g^{-1}) = (\phi(g))^{-1}$  for all  $g \in G$ .
  - (c) If  $K \leq G$ , then  $\phi(K) := \{\phi(k) \mid k \in K\}$  is a subgroup of  $H$ .
  - (d)  $\phi(G) := \{\phi(g) \mid g \in G\}$  (the image of  $\phi$ ) is a subgroup of  $H$ .
  - (e) If  $M \leq H$ , then  $\phi^{-1}(M) := \{g \in G \mid \phi(g) \in M\}$  is a subgroup of  $G$ .
19. **Lemma 6.3.** Let  $G$  be a group and  $H$ , a subgroup. Let  $g_1, g_2 \in G$ . Then, the following are equivalent:
- (a)  $g_1 H = g_2 H$ .
  - (b)  $H g_1^{-1} = H g_2^{-1}$ .
  - (c)  $g_1 H \subseteq g_2 H$ .
  - (d)  $g_2 \in g_1 H$ .
  - (e)  $g_1^{-1} g_2 \in H$ .
20. **Theorem 6.4.** Left  $H$ -cosets partition  $G$ .
21. **Lagrange's Theorem.** If  $G$  is a finite group and  $H$  is a subgroup of  $G$ , then  $|G| = |H| \cdot [G : H]$ , or  $[G : H] = \frac{|G|}{|H|}$ .
22. **Cor.** If  $G$  is a finite group and  $H$  is a subgroup of  $G$ , then  $|H|$  divides  $|G|$ .

23. **Cor. 6.13.** If  $G$  is a finite group and  $H \leq G$  and  $G \geq H \geq K$ , then  $[G : K] = [G : H] \cdot [H : K]$ .

---