

# 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  $[i] \cap [j] = \emptyset$ .
  - (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  $h_1h_2 \in H$ .
  - (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)  $g_1H = g_2H$ .
  - (b)  $Hg_1^{-1} = Hg_2^{-1}$ .
  - (c)  $g_1H \subseteq g_2H$ .
  - (d)  $g_2 \in g_1H$ .
  - (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  $[G : K] = [G : H] \cdot [H : K]$ .
- 
24. **Prop.**  $(\langle (123 \dots n) \rangle, \circ)$  is isomorphic to  $(\mathbb{Z}/n\mathbb{Z}, +)$ .
25. **Theorem 9.7. and 9.8** If  $G = (G, \star)$  is cyclic, then if:
- (a)  $G$  finite, then  $G$  is isomorphic to  $(\mathbb{Z}/n\mathbb{Z}, +)$ .
  - (b)  $G$  infinite, then  $G$  is isomorphic to  $(\mathbb{Z}, +)$ .
26. **Prop.** Assume  $G$  is abelian. Then every subgroup of  $G$  is normal.
27. **Prop.** Take  $G = \mathbb{Z}$ ,  $H = n\mathbb{Z}$ ,  $a, b \in \mathbb{Z}$ . Then  $aH \odot bH$  gives  $(a + n\mathbb{Z}) \odot (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$  is correctly defined.
28. **Theorem.** Let  $G$  be a group and  $H$  a normal subgroup. Then  $\odot$  (as in the above Prop.) defines a group structure on  $G/H$ , where  $G/H$  is called a quotient (factor) group.

29. **Prop.** Let  $\phi : G \rightarrow K$  be a homomorphism. Then,  $\ker \phi$  is a normal subgroup of  $G$ , with  $\ker \phi \trianglelefteq G$ .
30. **First Isomorphism Theorem.** Let  $\phi : G \rightarrow H$  be a homomorphism. Then  $G/\ker \phi \cong \text{Im} \phi$  and denote  $\Phi : G/\ker \phi \rightarrow \text{Im} \phi$  with  $g \cdot \ker \phi \mapsto \phi(g)$ .
31. **Theorem 9.27.** If  $G$  is an internal direct product of  $H$  and  $K$  (with  $H, K \leq G$ ), then,  $G \cong H \times K$ , where  $G$  represents an internal direct product and  $H \times K$  represents an external direct product.
32. **Fundamental Theorem of Finite Abelian Groups.** Every finite abelian group  $G$  is isomorphic to one of the following form:  $G \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_m^{a_m}\mathbb{Z}$  for  $p_1, \dots, p_m$  primes and  $a_1, \dots, a_m \in \mathbb{Z}_{>0}$ .
33. **Cor.** Any abelian group with 6 elements is isomorphic to  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ .
34. **Prop.** If  $G$  is a finite group with  $p$  elements (where  $p$  is prime), then  $G \cong \mathbb{Z}/p\mathbb{Z}$ .
35. **Prop.** If  $|G| = 4$ , then  $G$  is abelian.
36. **Prop.** If for any  $a \in G$ ,  $a^2 = e_G$ , then  $G$  is abelian.
37. **Prop.**  $\text{Sym}(\text{cube}) \cong S_4$ , so there are 24 symmetries of the cube, looking at the symmetry of the set of all 4 long diagonals inside the cube.
38. **Prop.** Let  $G$  be a group and  $X$  a set. Then, for each  $x \in X$ , we have  $\text{Stab}_G(x) \leq G$ .
39. **Prop.** If  $G$  acts on a set  $X$  and both  $G$  and  $X$  are finite, then  $|G| = |\text{Stab}_G(x)| \cdot |\text{orb}(x)|$  for all  $x \in X$ .
40. **Prop.** If  $G$  acts on  $X$ , then  $G$  acts by bijection, i.e.  $\{x \mid x \in X\} = \{g \circ x \mid x \in X\}$  (in bijection for any  $g \in G$ ).
41. **Prop.** For any sets  $A, B$  (that contain identity), with  $A \xrightarrow{\psi} B$  and  $A \xleftarrow{\phi} B$  with  $\phi \circ \psi = \text{id}_A$  and  $\psi \circ \phi = \text{id}_B$ , then both  $\phi$  and  $\psi$  are bijections.
42. **Prop.** The two definitions of actions are equivalent, i.e.  $\{\Phi : G \times X \rightarrow X\}$  (with properties 1 and 2 as in the (equivalent) definition of  $G$  acting on  $X$ ) is equal to the set  $\{\phi : G \rightarrow \text{Sym}(X)\}$ , where  $\phi$  is a homomorphism.
43. **Cayley's Theorem.** Every group is isomorphic to a subgroup of  $S_n$ .
44. **Lemma.** Let  $\lambda : G \rightarrow \text{Sym}(G)$  with be the left regular action of a group  $G$  on  $G$ . Then,  $\lambda$  is injective.
45. **Burnside's Lemma.** Let  $G$  be a finite group with  $G$  acting on a finite set  $X$ . The number of  $G$ -orbits in  $X$  is  $\frac{1}{|G|} \cdot \sum_{g \in G} |X^g|$ , where  $|X^g|$  is the number of elements in  $X$  fixed by the action of  $g \in G$ .
46. **Theorem.** The set of normal subgroups in  $G$  is equal to the set of all  $\ker \phi$  where  $\phi : G \rightarrow H$  is a homomorphism.

47. **Prop.**  $\ker \phi$  is an ideal in  $R$  for any ring homomorphism  $\phi : R \rightarrow S$ .
48. BELOW ARE ADDITIONAL THMS FOR MT2
49. **Prop 16.8.** Let  $R$  be a ring with  $a, b \in R$ . Then:
- (a)  $a0 = 0a = 0$ .
  - (b)  $a(-b) = (-a)b = -ab$ .
  - (c)  $(-a)(-b) = ab$ .
50. **Prop 16.10.** Let  $R$  be a ring and  $S$  a subset of  $R$ . Then  $S$  is a subring of  $R$  iff:
- (a)  $S \neq \emptyset$ .
  - (b)  $rs \in S$  for all  $r, s \in S$ .
  - (c)  $r - s \in S$  for all  $r, s \in S$ .
51. **Prop. 16.15. Cancellation Law.** Let  $D$  be a commutative ring with identity. Then  $D$  is an integral domain iff for all nonzero elements  $a \in D$  with  $ab = ac$ , we have  $b = c$ .
52. **Theorem 16.16.** Every finite integral domain is a field.
53. **Prop. 16.22.** Let  $\phi : R \rightarrow S$  be a ring homomorphism. Then:
- (a) If  $R$  is a commutative ring, then  $\phi(R)$  is a commutative ring.
  - (b)  $\phi(0) = 0$ .
  - (c) Let  $1_R$  and  $1_S$  be the identities for  $R$  and  $S$ , respectively. If  $\phi$  is onto, then  $\phi(1_R) = 1_S$ .
  - (d) If  $R$  is a field and  $\phi(R) \neq \{0\}$ , then  $\phi(R)$  is a field.
54. **Theorem 16.25.** Every ideal in the ring of integers  $\mathbb{Z}$  is a principal ideal.
55. **Prop. 16.27.** The kernel of any ring homomorphism  $\phi : R \rightarrow S$  is an ideal in  $R$ .
56. **First Ring Isomorphism Theorem.** Take  $\psi : R \rightarrow S$  a ring homomorphism. Then  $\ker \psi$  is an ideal of  $R$  and  $R/\ker \psi \cong \text{Im} \psi$ , and let  $\Psi : R/\ker \psi \rightarrow \text{Im} \psi$  with  $r + \ker \psi \mapsto \psi(r)$ .
- 
57. **Prop.** If  $T$  is a field, then its only ideals are  $\{0\}$  and  $T$ .
58. **Theorem 16.35.**  $R/I$  is a field iff  $I$  is a maximal ideal in  $R$ .
59. **Prop.** For a given ring, the set of its units and the set of its zero divisors are disjoint.
60. **Prop.**  $R/I$  is an integral domain iff  $I$  is a prime ideal.

61. **Division Algorithm.** Let  $a, b \in \mathbb{Z}$ , with  $b > 0$ . Then there it exists unique integers  $q, r$  such that  $a = bq + r$ , where  $0 \leq r < b$ .
62. **Theorem 2.10.** Let  $a, b$  be nonzero integers. Then there exists integers  $r, s$  such that  $\gcd(a, b) = ra + sb$  and  $\gcd(a, b)$  is unique.
63. **Fundamental Theorem of Arithmetic.** Let  $n \in \mathbb{Z}$  with  $n > 1$ . Then  $n = p_1 \cdots p_k$  where  $p_i$  is prime. This factorization is unique.
64. **Theorem 17.6.** If  $a(x), b(x) \in F[x]$ , then there exists unique  $q(x), r(x) \in F[x]$  such that:
- (a)  $a(x) = q(x)b(x) + r(x)$ .
  - (b)  $\deg(r(x)) < \deg(b(x))$ .
65. **Cor. 17.8.** If  $F$  is any field, then  $\alpha \in F$  is a zero of  $f(x) \in F[x]$  iff  $(x - \alpha) \mid f(x)$ .
66. **Cor. 17.9.** If  $F$  is any field and  $f(x) \in F[x]$  has degree  $n$ , then  $f(x)$  has at most  $n$  zeros in  $F$ .
67. **Prop.**  $\mathbb{Z}[i]$  is a commutative ring with 1 but not a field.
68. **Lemma.** Units in  $\mathbb{Z}[i]$  are  $\pm 1, \pm i$  and  $\mathbb{Z}[i]$  is an integral domain.
69. **Prop.**  $N(xy) = N(x)N(y)$  for  $x, y \in \mathbb{Z}[i]$ .
70. **Theorem (Division Algorithm).** If  $\alpha, \beta \in \mathbb{Z}[i]$ , with  $\beta \neq 0$ , then there exist  $q, r \in \mathbb{Z}[i]$  (not necessarily unique) such that  $\alpha = q \cdot \beta + r$  and  $0 \leq N(r) < N(\beta)$ .
71. **Lemma.**  $\mathbb{Z}[\sqrt{-5}]$  is a commutative with 1 but not a field.
72. **Lemma.**
- (a) Units in  $\mathbb{Z}[\sqrt{-5}]$  are  $\pm 1$ .
  - (b)  $\mathbb{Z}[\sqrt{-5}]$  is an integral domain.
73. **Prop.**  $N(xy) = N(x)N(y)$  for all  $x, y \in \mathbb{Z}[\sqrt{-5}]$ .
74. **Lemma.** Let  $R$  be an integral domain. Then every prime is irreducible.
75. **Prop.**  $3 = 3 + 0 \cdot \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$  is irreducible but not prime.
76. **Lemma.** Let  $R$  be an integral domain. Then  $\langle u \rangle = R$  iff  $u$  is a unit in  $R$ .
77. **Lemma.** Let  $R$  be an integral domain. Take  $r \in R$  (non-unit). Then  $\langle r \rangle$  is prime iff  $r$  is a prime.
78. **Lemma.** If  $I = \langle a \rangle$  and  $J = \langle b \rangle$ , then  $I \cdot J = \langle ab \rangle$ , where  $I, J$  are ideals in an integral domain  $R$ .

79. **Theorem.** If  $R = \mathbb{Z}$  and  $x_1, \dots, x_n \in \mathbb{Z}$ , then  $\langle x_1, \dots, x_n \rangle := \{a_1x_1 + \dots + a_nx_n \mid a_i \in \mathbb{Z} \forall i\} = \langle \gcd(x_1, \dots, x_n) \rangle$ .
80. **Prop.**  $\mathbb{Z}[\sqrt{-5}]$  is not a principal ideal domain, so not every ideal is principal.

---

Extra

---

81. **Prop.** Let  $R = \mathbb{Z}[\sqrt{-5}]$ . Then, for norm:
- (a)  $N(\alpha) = 0$  iff  $\alpha = 0$ .
  - (b)  $\alpha$  is a unit iff  $N(\alpha) = 1$  ( $\pm 1$  are the only units of  $\mathbb{Z}[\sqrt{-5}]$ ).
  - (c) If  $N(\alpha)$  is prime, then  $\alpha$  is irreducible.
82. **Prop.** Every maximal ideal of a commutative ring with identity is prime.
83. **Fundamental Theorem of Ideal Theory.** Let  $I$  be a nonzero proper ideal of  $\mathbb{Z}[\sqrt{-5}]$ . Then there exists a unique (up to order) list of prime ideals  $P_1, \dots, P_k$  of  $\mathbb{Z}[\sqrt{-5}]$  such that  $I = P_1 \cdots P_k$ .
84. **Prop.** Let  $\alpha$  be a nonzero nonunit element in  $\mathbb{Z}[\sqrt{-5}]$ . Then  $\alpha \in \mathbb{Z}[\sqrt{-5}]$  is irreducible iff
- (a)  $\langle \alpha \rangle$  is a prime ideal (thus  $\alpha$  is prime), or
  - (b)  $\langle \alpha \rangle = P_1P_2$  where  $P_1$  and  $P_2$  are nonprincipal prime ideals of  $\mathbb{Z}[\sqrt{-5}]$ .
85. **Theorem.** If  $\alpha$  is a nonzero element of  $\mathbb{Z}[\sqrt{-5}]$ , and  $\beta_1, \dots, \beta_s; \gamma_1, \dots, \gamma_t$  are irreducible in  $\mathbb{Z}[\sqrt{-5}]$  with  $\alpha = \beta_1 \cdots \beta_s = \gamma_1 \cdots \gamma_t$ , then  $s = t$ .

- 
86. **Theorem.** Let  $F$  be a field. Then  $F[x]$  is a PID.
87. **Theorem.** Let  $p(x) \in F[x]$ . Then  $\langle p(x) \rangle$  is maximal iff  $p(x)$  is irreducible.
88. **Prop.** In  $F[x]$ , prime ideals iff maximal ideals.
89. **Lemma.** If  $E \geq F$  is a field extension, then  $E$  is an  $F$ -vector space.
90. **Prop.**  $F[\alpha] \cong F[x]/\langle p(x) \rangle$  for irreducible  $p(x)$ .
91. **Splitting field algorithm.** Let  $F$  be a field and  $p(x) \in F[x]$  irreducible. To find the splitting field  $F[p(x)]$ , notice  $F_1 := F[x]/\langle p(x) \rangle$  and  $p(x) = (x - \alpha)q(x) \in F_1[x]$ . Put  $F_2 := F_1[x]/\langle q(x) \rangle$ , and so on.
92. **Prop.** Let  $F = K(\alpha_1, \alpha_2)$  be a field extension. Then  $[F : K] = [F : K(\alpha_1)] \cdot [K(\alpha_1) : K]$ .
93. **Prop.**  $\{\text{id}, \text{conj}\}$  are all the automorphisms of  $\mathbb{C}$  over  $\mathbb{R}$ .