

Math 113 Definitions.

1. **Set.** A set is an unordered collection of elements.
2. **Map.** A map from  $X$  to  $Y$  is  $f : X \rightarrow Y$  (a rule that assigns elements to  $Y$  to elements in  $X$ ). So, for any  $x \in X$  there exists a unique  $y \in Y$  such that  $f(x) = y$ .
3. **Cartesian Product.** The Cartesian product of  $X$  and  $Y$  is the set  $X \times Y = \{(x, y) \mid x \in X, y \in Y\}$ .
4. **Equivalence Relation.** An equivalence relation  $R, \sim$  on  $X$  is a subset  $R \subseteq X \times X$  such that
  - (a) Reflexive.  $((x, x) \in R \text{ for all } x \in X)$ .
  - (b) Symmetric.  $(\text{if } (x, y) \in R, \text{ then } (y, x) \in R)$ .
  - (c) Transitive.  $(\text{if } (x, y) \in R \text{ and } (y, z) \in R, \text{ then } (x, z) \in R)$ .
5. **Equivalence Class.** Let  $X$  be a set and  $R$  be an equivalence relation on  $X$ . Then, an equivalence class of  $x \in X$  is the set  $[x] = [x]_R = [x]_\sim = \{a \in X \mid x \sim a\}$ .
6.  $\mathbb{Z}/m\mathbb{Z}$ . The set of distinct equivalence classes of  $\equiv \pmod{n}$  is  $\mathbb{Z}/m\mathbb{Z}$ .
7. **Group.** A group  $G$  (denote:  $(G, \star)$ ) is a set  $G$  with a closed binary operation  $\star : G \times G \rightarrow G$  such that:
  - (a) Associativity:  $(a \star b) \star c = a \star (b \star c)$  for all  $a, b, c \in G$ .
  - (b) Identity: There exists an  $e \in G$  such that for any  $a \in G$ , we have  $a \star e = e \star a = a$ .
  - (c) Inverse: For any  $a \in G$ , there exists an  $a^{-1} \in G$  such that  $a \star a^{-1} = a^{-1} \star a = e$ .
8. **Symmetric Group.** The symmetric group on  $n$  letters is  $S_n$ .
9. **Disjoint Cycles.** Two cycles  $(a_1, \dots, a_k)$  and  $(b_1, \dots, b_l)$  are disjoint if  $a_i \neq b_j$  for all  $i, j$ .
10. **Transpositions.** The simplest permutation is a cycle of length 2, which is called a transposition.
11. **Even, Odd Permutations.** A permutation is even if it can be expressed as an even number of transpositions. A permutation is odd if it can be expressed as an odd number of transpositions.
12. **Subgroup.** A subgroup  $H$  of a group  $G$  is a subset  $H$  of  $G$  such that when the group operation of  $G$  is restricted to  $H$ , then  $H$  is a group.
13. **Trivial/Proper Subgroup.** The trivial subgroup of a group  $G$  is  $\{e\}$  and a proper subgroup is a subgroup  $H$  of  $G$  where  $H$  is a proper subset of  $G$ .

14. **General/Special Linear Group.**  $GL_2(\mathbb{R})$  is the set of 2x2 invertible matrices with real entries.  $SL_2(\mathbb{R})$  is the set of 2x2 invertible matrices with real entries and with determinant 1.
  15. **Cyclic Group.** A cyclic group is a group generated by one element.
  16. **Isomorphism.** An isomorphism is a homomorphism which is bijective.
  17. **Kernel of homomorphism.** If  $\phi : G \rightarrow H$  is a homomorphism, then  $\ker \phi$  is the pre-image of  $e_H \in H$ , that is,  $\ker \phi = \{g \in G \mid \phi(g) = e_H\}$ .
  18. **Coset.** Let  $(G, \star) \geq (H, \star)$  and  $g \in G$ . Then, an  $H$ -coset of  $g$  is a (sub)set of  $G$  where  $gH = g \star H = \{g \star h \mid h \in H\}$  (left coset) and  $Hg = \{h \star g \mid h \in H\}$  (right coset).
  19. **Index.** A set of distinct equivalence classes with respect to  $\sim_H$  is  $G/H$ , a quotient of  $G$  by  $H$ . Then,  $|G/H| = [G : H]$  is the index of  $H$  in  $G$ .
  20. The following are definitions listed in the homeworks:
    - (a) Group of units in  $\mathbb{Z}/n\mathbb{Z}$  is the set  $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z}^\times := \{[a] \in \mathbb{Z}/n\mathbb{Z} \mid \exists [b] \in \mathbb{Z}/n\mathbb{Z} \text{ with } [a] \times [b] = [1]\}$ .
    - (b) If  $G$  is a group, then the center of  $G$  is the set  $Z(G) := \{a \in G \mid ga = ag \forall g \in G\}$ .
    - (c)  $\mathbb{C}^\times$  is the set of nonzero complex numbers.
    - (d)  $\mathbb{R}^\times$  is the set of nonzero real numbers.
    - (e)  $GL(n, K)$  is the set of  $n \times n$  invertible matrices with entries in  $K$ .
    - (f) If  $G$  is a group, then the torsion subgroup of  $G$  is called  $G_T$ , which is the set of all elements of  $G$  with finite order.
    - (g) The Klein four-group is  $V$  is a subgroup of  $S_4$  and consists of  $V = \{\text{id}, (12), (34), (12)(34)\}$ .
- 
21. **Dihedral group.** This is the group of symmetries on a regular  $n$ -gon with  $r$  being rotation  $s$  flip. We have  $r^n = \text{id}$ ,  $s^2 = \text{id}$ , and  $sr = rs^{-1}$ .
  22. **(External) Direct Product** Let  $G = (G, \star)$  and  $H = (H, \circ)$  be groups. Then,  $G \times H = \{G \times H, (\star, \circ)\}$ .
  23. **Normal Subgroup.** Let  $G$  be a group and  $H$  a subgroup of  $G$ . Then  $H$  is a normal subgroup (write  $H \trianglelefteq G$ ) iff for all  $g \in G$ ,  $gH = Hg$ , or equivalently, for all  $h \in H$ ,  $ghg^{-1} \in H$  for all  $g \in G$ .
  24. **Quotient (factor) group.** The quotient group of a group  $G$  and a normal subgroup  $N$  of  $G$  is the group  $G/N$  (where  $G/N$  is the group of cosets of  $N$  in  $G$ ) under the operation  $(aN)(bN) = abN$ .

25. **Internal Direct Product.** Let  $G$  be a group and  $H, K \leq G$ .  $G$  is an internal direct product of  $H$  and  $K$  iff:
- (a)  $G = H \cdot K := \{h \cdot k \mid h \in H, k \in K\}$ .
  - (b)  $H \cap K = \{e_G\}$  (“as small as possible”).
  - (c)  $h \cdot k = k \cdot h$  for all  $h \in H, k \in K$ .
26. **Simple group.** A group  $G$  is simple if the only normal subgroups are  $\{e_G\}$  and  $G$ .
27. **Symmetry.** A symmetry of  $X$  is a bijective map  $\sigma : X \rightarrow X$  preserving the structure where  $X$  is some set with some additional structure.
28. **Group of permutations on a set  $X$ .**  $G$  is a group of permutations on a set  $X$  if  $\phi : G \rightarrow \text{Sym}(X) = S_X = S_{|X|}$  is a homomorphism that is 1-1.
29.  **$G$  acts on a set  $X$ .**  $G$  acts on a set  $X$  is a homomorphism  $\phi : G \rightarrow \text{Sym}(X)$ .
30. **Stabilizer of  $x \in X$ .** Let  $G$  be a group and  $X$  a set. Then, the stabilizer of  $x \in X$  is  $\text{Stab}_G(x) = \{g \in G \mid g(x) = x\}$ , which are elements of  $g$  that preserve  $x \in X$ .
31. **Orbit of  $x \in X$ .** Take  $x \in X$ . Then the orbit of  $x$  is  $\text{orb}_G(x) = \mathcal{O}_G(x) = \mathcal{O}(x) = \{g(x) \mid g \in G\} \subseteq X$ .
32.  **$G$  acts on a set  $X$  (equivalent) def.** A group  $G$  acts on a set  $X$  iff  $\Phi : G \times X \rightarrow X$  with  $(g, x) \mapsto \Phi(g, x) = g \circ x$  such that:
- (a) for all  $x \in X$ ,  $\Phi(e_G, x) = x$ .
  - (b) for all  $x \in X$ ,  $g, h \in G$ ,  $\Phi(gh, x) = \Phi(g, \Phi(h, x))$ .
33. **Left regular action of  $G$  on  $G$ .** Define  $\Lambda : G \times G \rightarrow G$  be a group action, where  $G$  is a group (and a set) such that  $(g, h) \mapsto g \circ h$ . Equivalently, the left regular action of  $G$  on  $G$  is defined as the homomorphism  $\lambda : G \rightarrow \text{Sym}(G)$  such that  $g \mapsto (\lambda_g : h \mapsto \lambda_g(h) = g \circ h)$ , where  $\lambda_g$  is a permutation on the set  $G$  for  $g \in G$ .
34. **Ring.** A ring  $R = (R, +, \times)$  is a set with two closed binary operations  $(+)$  and  $(\times)$  such that:
- (a)  $(R, +)$  is an abelian group.
  - (b)  $(R, \times)$  is associative.
  - (c) Both distributive properties hold, i.e.  $a \times (b + c) = (a \times b) + (a \times c)$  and  $(a + b) \times c = (a \times c) + (b \times c)$  for all  $a, b, c \in R$ .
35.  **$R^\times$ .** Let  $R$  be a ring. Then, we define  $R^\times = \{a \in R \mid \exists b \in R : ab = 1_R\}$ , where  $(R^\times, \times)$  is a group, possibly abelian.
36. **Field.** Let  $R = (R, +, \times)$  be a commutative ring with  $1_R$  being the multiplicative identity. Then if  $R^\times = R \setminus \{0\}$ , then  $R$  is a field.

37. **Ring Homomorphism.** Let  $R = (R, +, \times)$  and  $S = (S, +, \times)$  be rings. Then a map  $\phi : R \rightarrow S$  is a homomorphism of rings iff  $\phi(a +_R b) = \phi(a) +_S \phi(b)$  and  $\phi(a \times_R b) = \phi(a) \times_S \phi(b)$ . Additionally, axiomatically,  $\phi(1_R) = 1_S$  and a property is  $\phi(0_R) = 0_S$ . Also, define  $\ker \phi := \{r \in R \mid \phi(r) = 0_S\}$ .
38. BELOW IS ADDITIONAL DEFS FOR MT2
39. A **ring with unity (or with identity)** is a ring  $R$  that has multiplicative identity.
40. A **commutative ring** is a ring  $R$  that has multiplicative commutativity.
41. An **integral domain** is a commutative ring  $R$  with identity such that for all  $a, b \in R$   $ab = 0$  implies  $a = 0$  or  $b = 0$ .
42. A **division ring** is a ring  $R$  that has multiplicative inverse for all nonzero  $a \in R$ .
43. A **zero divisor** of a commutative ring  $R$  is an  $a \in R$  ( $a \neq 0$ ) such that there exists a nonzero  $b \in R$  such that  $ab = 0$ .
44. The **ring of quaternions** is the set  $\mathbb{H} = \{a + b\hat{i} + c\hat{j} + d\hat{k} \mid a, b, c, d \in \mathbb{R}\}$ , where  $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \hat{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \hat{j} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \hat{k} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ .
45. A **field** is a commutative division ring.
46. The **characteristic** of a ring  $R$  is the least positive integer  $n$  such that  $nr = 0$  for all  $r \in R$ . If no such  $n$  exists, the characteristic of  $R$  is defined to be 0. (denote the characteristic of  $R$  by  $\text{char}R$ ).
47. A **ring homomorphism** is a map  $\phi : R \rightarrow S$  (where  $R, S$  are rings) such that  $\phi(a + b) = \phi(a) + \phi(b)$  and  $\phi(ab) = \phi(a)\phi(b)$  for all  $a, b \in R$ .
48. A **ring isomorphism** is a bijective map  $\phi : R \rightarrow S$  where  $R, S$  are rings.
49. The **kernel** of a ring homomorphism  $\phi : R \rightarrow S$  is the set  $\ker \phi := \{r \in R \mid \phi(r) = 0\}$ .
50. An **evaluation homomorphism** is a ring homomorphism of the form  $\phi_\alpha : C[a, b] \rightarrow \mathbb{R}$  or other such related homomorphisms.
51. An **ideal** of a ring  $R$  is a subring  $I$  such that
- $(I, +)$  is a subgroup of  $(R, +)$ .
  - if  $a \in I$  and  $r \in R$ , then  $ar, ra \in I$ .
52. The **trivial ideals** of a ring  $R$  are the subrings  $\{0\}$  and  $R$ .
53. A **principal ideal** of a commutative ring  $R$  (with identity) is an ideal of the form  $\langle a \rangle = \{ar \mid r \in R\}$ .

54. A **two-sided ideal**  $I$  is a subring of a ring  $R$  such that  $rI \subset I$  and  $Ir \subset I$  for all  $r \in R$ .
55. A **one-sided ideal**  $I$  is a subring of a ring  $R$  is one such that  $rI \subset I$  for all  $r \in R$  (a **left ideal**) or  $Ir \subset I$  for all  $r \in R$  (a **right ideal**).
56. **Quotient ring.** Let  $R$  be a ring and  $I$  a two-sided ideal of  $R$ . Then the quotient ring  $R/I$  is defined to be the set of all cosets of  $I$  with respect to  $+$  and  $\times$ .
57. **Natural/canonical homomorphism.** The map  $\phi : R \rightarrow R/I$  is called the natural/canonical homomorphism.
- 

58. **proper ideal.**  $I \subseteq R$  is a proper ideal of  $R$  iff  $I \neq \{0_R\}$  and  $I \neq R$ .
59. **Integral domain.** A commutative ring  $R$  with  $1_R$  is an integral domain if there are no (nonzero) zero-divisors.
60. **Prime ideal.** An ideal  $I$  of a ring  $R$  is a prime ideal if  $ab \in I$  means  $a \in I$  or  $b \in I$ .
61. **Prime.** Let  $p \in D$ , where  $D$  is an integral domain and  $p$  a non-unit.  $p$  is prime iff if  $p \mid ab$ , then  $p \mid a$  or  $p \mid b$ .
62. **Irreducible.** Let  $x \in D$ , where  $D$  is an integral domain and  $x$  a non-unit.  $x$  is irreducible iff if  $x = ab$  means  $a$  is a unit or  $b$  is a unit.
63. **Principal ideal domain (PID).** A principal ideal is an integral domain in which every ideal is a principal ideal.
64. **Unique factorization domain (UFD).** An integral domain  $D$  is a unique factorization domain (UFD) if:
- (a) Let  $a \in D$  such that  $a \neq 0$  and  $a$  is a non-unit. Then  $a$  can be written as the product of irreducible elements of  $D$ .
  - (b) Let  $a = p_1 \cdots p_r = q_1 \cdots q_s$ , where  $p_i, q_k$  are irreducible. Then  $r = s$  and there is a  $\pi \in S_r$  such that  $p_i$  and  $q_{\pi(j)}$  are associates for  $j = 1, \dots, r$ .
65. **Euclidean domain.** Let  $D$  be an integral domain such that there is a function  $v : D \setminus \{0\} \rightarrow \mathbb{N}$  such that:
- (a) If  $a, b$  are nonzero elements of  $D$ , then  $v(a) \leq v(ab)$ .
  - (b) Let  $a, b \in D$  and suppose  $b \neq 0$ . Then There exist elements  $q, r \in D$  such that  $a = bq + r$  and either  $r = 0$  or  $v(r) < v(b)$ .

Then  $D$  is a Euclidean domain.

66. **Gaussian Integers.** The set of Gaussian integers is the set  $\{a + bi \mid a, b \in \mathbb{Z}, i^2 = -1\} =: \mathbb{Z}[i]$ .
67. **Norm.** Let  $z \in \mathbb{Z}[i]$ . Then we define the norm of  $z$  to be  $N(z) = z \cdot \bar{z}$ , or if  $z = a + bi \in \mathbb{Z}[i]$ , then  $N(z) = a^2 + b^2$ .