Exam I Review

Except part V, all the other parts come from the *review* in each lecture slide.

I. (i) (a,b) & $[a,b]$ $\dashrightarrow$ $(a,b)\cdot[a,b]=ab$
(ii) $(a,b)|(am+bn)$, linear combination of a and b
(iii) Division Algorithm $\dashrightarrow$ The Euclidean Algorithm (matrix form)
(iv) $(a,b)=1 \Leftrightarrow am+bn=1$ for some $m,n\in\mathbf{Z}$
(v) If $b|ac$ and $(a,b)=1 \Rightarrow b|c$
(vi) $a\equiv b \pmod n \Leftrightarrow n|(a-b) \Leftrightarrow a=b+qn \Leftrightarrow [a]_n=[b]_n$
(vii) If $ac\equiv ad \pmod n$ and $(a,n)=1$ (i.e., $a\in\mathbf{Z}_n^\times$) $\Rightarrow c\equiv d \pmod n$
(viii) Divisor of zero **v.s.** Unit (Cancellation law $\checkmark$) in $\mathbf{Z}_n$
(ix) Linear congruence $ax\equiv b \pmod n$ has a solution $\Leftrightarrow (a,n)|b$
(x) System of congruences: Chinese Remainder Theorem
(xi) For $[a]\in\mathbf{Z}_n^\times$, find $[a]^{-1}$:
(1) the Euclidean algorithm (2) successive powers (3) trial and error
(xii) Euler's totient function $\varphi(n)=\#\{a\colon (a,n)=1, 1\le a\le n\}=\#|\mathbf{Z}_n^\times|$
(xiii) Euler's theorem $\dashrightarrow$ Fermat's "little" theorem

---

II. (i) Permutation $\sigma\in\mathrm{Sym}(S)$ (or S_n)
(ii) $\#|S_n|=n!$
(iii) Composition (Product) $\sigma\tau$ & Inverse σ^{-1}
(iv) Cycle of length k: $\sigma=(a_1a_2\cdots a_k)$ has order k.
(v) Disjoint cycles are commutative
(vi) $\sigma\in S_n$ can be written as a *unique* product of disjoint cycles.
(vii) The order of σ is the **lcm** of the lengths (orders) of its disjoint cycles.
(viii) A **transposition** is a cycle (a_1a_2) of length two.
(ix) $\sigma\in S_n$ can be written as a product of transpositions. (NOT unique)
(x) Even Permutation & Odd Permutation
(xi) A cycle of odd length is even. & A cycle of even length is odd.

III. (i) Group $(G,*)$ $\begin{cases}\text{i)} & \text{Closure} \rightsquigarrow *\\ \text{ii)} & \text{Associativity} \rightsquigarrow (\cancel{\checkmark})\\ \text{iii)} & \text{Identity: Uniqueness by Associativity}\\ \text{iv)} & \text{Inverses: Uniqueness by Associativity}\end{cases}$

eg. $(\mathbf{R}^\times,\cdot)$, $(\mathrm{Sym}(S),\circ)$, $(M_n(\mathbf{R}),+_{\text{matrix}})$, $(\mathrm{GL}_n(\mathbf{R}),\cdot_{\text{matrix}})$
(ii) Cancellation law
(iii) Abelian group: eg. $(\mathbf{Z},+)$, $(\mathbf{Z}_n,+_{[\ ]})$, $(\mathbf{Z}_n^\times,\cdot_{[\ ]})$
(iv) Finite group (**order**) v.s. Infinite group
(v) Conjugacy: $x\sim y$ if $y=axa^{-1}\rightsquigarrow$ Equivalence relation

---

IV. (i) Subgroup H: $\begin{cases}\text{Closure}\\ \text{Identity}\\ \text{Inverses}\end{cases}$ (*no worry about* associativity)

- Alternative way: H is nonempty and $ab^{-1}\in H$ for all $a,b\in H$

- If H is finite, then H is nonempty and $ab \in H$ for all $a, b \in H$
- e.g.: $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$; $\mathbf{R}^+ \subseteq \mathbf{R}^\times$; $n\mathbf{Z} \subseteq \mathbf{Z}$; $\mathrm{SL}_n(\mathbf{R}) \subseteq \mathrm{GL}_n(\mathbf{R})$.

(ii) Cyclic subgroup $\langle a \rangle$ is the **smallest** subgroup of G containing $a \in G$.
e.g.: $\langle i \rangle \subseteq \mathbf{C}^\times$ & $\langle 2i \rangle \subseteq \mathbf{C}^\times$; $\langle (123) \rangle \subseteq S_3$ & $\langle (12) \rangle \subseteq S_3$.

(iii) G is cyclic if $G = \langle a \rangle$.
e.g.: $\mathbf{Z}$, $\mathbf{Z}_n$, $\mathbf{Z}_5^\times$. not e.g.: $\mathbf{Z}_8^\times$, S_3.

(iv) $o(a) = |\langle a \rangle|$. If $o(a) = n$ is finite, then $a^k = e \Leftrightarrow n|k$.

(v) **Lagrange's Theorem:** If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \mid n$.
- $o(a)|n$ for any $a \in G$. $\rightsquigarrow a^n = e \dashrightarrow$ Euler's theorem
- Any group of prime order is cyclic (and so abelian).
$\rightsquigarrow$ Any group of order 2, 3, or 5 must be cyclic.

V. (i) Groups of order 4 are abelian: cyclic [$\mathbf{Z}_4$] **vs.** non-cyclic [$\mathbf{Z}_8^\times$]

(ii) Groups of order 6: abelian (cyclic) [$\mathbf{Z}_6$] **vs.** nonabelian [S_3]

(iii) Product of two subgroups: HK is not always a subgroup of G.
If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G.

(iv) If G is abelian, then the product of any two subgroups is again a subgroup.
[$a\mathbf{Z} + b\mathbf{Z} = (a, b)\mathbf{Z}$]

(v) If G is a finite group, then $|HK| = |H||K|/|H \cap K|$.

(vi) Direct product of two groups: $G_1 \times G_2$ is a group under a new defined operation.

(vii) $o((a_1, a_2)) = \mathrm{lcm}[o(a_1), o(a_2)]$

(viii) If G_1, G_2 are finite groups, then $|G_1 \times G_2| = |G_1| \cdot |G_2|$.

(ix) $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic if and only if $\gcd(n, m) = 1$.

(x) Subgroup generated by S: $\langle S \rangle$ is the smallest subgroup that contains S.

(xi) Definition of a field and New groups defined over a filed F. [$\mathbf{Z}_p$; $\mathrm{GL}_n(F)$]

Other resources for review: Your class notes & Lecture Slides/Recordings & Homework

Good luck for the test!