# Some Additional Practice Problems for Final Exam

Review Lecture Slides/Recordings & Homework Assignments

*Good luck for the final !*

(1) Find $\gcd(7605, 5733)$, and express it as a linear combination of 7605 and 5733.

$$\begin{bmatrix} 1 & 0 & 7605 \\ 0 & 1 & 5733 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 1872 \\ 0 & 1 & 5733 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 1872 \\ -3 & 4 & 117 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 49 & -65 & 0 \\ -3 & 4 & 117 \end{bmatrix}$$

Thus $\gcd(7605, 5733) = 117$, and $117 = (-3) \cdot 7605 + 4 \cdot 5733$.

(2) Solve the congruence $24x \equiv 168 \pmod{200}$.

$d = \gcd(24, 200) = 8 | 168 \Rightarrow 3x \equiv 21 \pmod{25}$ and we have $3 \cdot 17 \equiv 1 \pmod{25}$. Thus, $x \equiv 21 \cdot 17 \equiv 7 \pmod{25}$, i.e., $x \equiv 7, 32, 57, 82, 107, 132, 157, 182 \pmod{200}$.

(3) Solve the system of congruences $2x \equiv 9 \pmod{15}$ $x \equiv 8 \pmod{11}$.

Since $2 \cdot 8 \equiv 1 \pmod{15}$, $x \equiv 9 \cdot 8 \equiv 12 \pmod{15}$. And $3 \cdot 15 + (-4) \cdot 11 = 1$. By Chinese Remainder Theorem, we have $x \equiv 12 \cdot (-44) + 8 \cdot (45) \pmod{15 \cdot 11}$, i.e.,

$$x \equiv -3 \equiv 162 \pmod{165}.$$

(4) Let $\sigma = (13579)(126)(1253)$. Find its order and its inverse. Is $\sigma$ even or odd?

$\sigma = (163279)(4)(5)(8) = (163279)$. So $o(\sigma) = 6$ and $\sigma^{-1} = (972361) = (197236)$. And it is easy to see that $\sigma$ is odd.

(5) Let $(G, \cdot)$ be a group and let $a \in G$. Define a new operation $*$ on the set $G$ by

$$x * y = x \cdot a \cdot y, \text{ for all } x, y \in G.$$

Show that $G$ is a group under the operation $*$.

(i) Closure (well-defined): Trivial.

(ii) Associativity: For all $x, y, z \in G$, we have

$$(x * y) * z = (x \cdot a \cdot y) * z = (x \cdot a \cdot y) \cdot a \cdot z = x \cdot a \cdot (y \cdot a \cdot z) = x * (y * z).$$

(iii) Identity: The identity element is $a^{-1}$. In particular, for any $x \in G$ we have

$$a^{-1} * x = a^{-1} \cdot a \cdot x = x \quad \text{and} \quad x * a^{-1} = x \cdot a \cdot a^{-1} = x.$$

(iv) Inverses: For any $x \in G$, its inverse is $(a \cdot x \cdot a)^{-1}$. In particular, we have

$$x * (a \cdot x \cdot a)^{-1} = x \cdot a \cdot a^{-1} \cdot x^{-1} \cdot a^{-1} = a^{-1}$$
$$(a \cdot x \cdot a)^{-1} * x = a^{-1} \cdot x^{-1} \cdot a^{-1} \cdot a \cdot x = a^{-1}$$

(6) For each binary operation $*$ given below, determine whether or not $*$ defines a group structure on the given set. If not, list the group axioms that fail to hold.

(a) Define $*$ on $\mathbf{Z}$ by $a * b = \min\{a, b\}$.

The operation is associative, but has no identity element.

(b) Define $*$ on $\mathbf{Z}^+$ by $a * b = \max\{a, b\}$.

The operation is associative, but has no identity element.

(c) Define $*$ on $\mathbf{Z}$ by $x * y = x^2y^3$.

The associative law fails, and there is no identity element.

(d) Define $*$ on $\mathbf{Z}^+$ by $x * y = x^y$.

The associative law fails, and there is no identity element.

(e) Define $*$ on $\mathbf{R}$ by $x * y = x + y - 1$.

Yes. $(\mathbf{R}, *)$ is a group.

(f) Define $*$ on $\mathbf{R}^\times$ by $x * y = xy + 1$.

The operation is not a binary operation (since closure fails).

(7) Show that if $|G| = pq$, where $p \neq q$ are prime numbers, then every proper nontrivial subgroup of $G$ is cyclic.

*Proof.* Let $H$ be a proper nontrivial subgroup of $G$. By Lagrange's Theorem, $|H|$ has to be $p$ or $q$ since $H$ is a proper nontrivial subgroup. And so $H$ is cyclic. □

(8) Let $K$ be the following subset of $\mathrm{GL}_2(\mathbf{R})$.

$$K = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbf{R}) \middle| a = d, c = -2b \right\}$$

Show that $K$ is a subgroup of $\mathrm{GL}_2(\mathbf{R})$.

(i) Nonempty: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in K$.

(ii) For any $\begin{bmatrix} a_1 & b_1 \\ -2b_1 & a_1 \end{bmatrix}, \begin{bmatrix} a_2 & b_2 \\ -2b_2 & a_2 \end{bmatrix} \in K$, to show $\begin{bmatrix} a_1 & b_1 \\ -2b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ -2b_2 & a_2 \end{bmatrix}^{-1} \in K$.

$$\begin{aligned} \begin{bmatrix} a_1 & b_1 \\ -2b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ -2b_2 & a_2 \end{bmatrix}^{-1} &= \frac{1}{a_2^2 + 2b_2^2} \begin{bmatrix} a_1 & b_1 \\ -2b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & -b_2 \\ 2b_2 & a_2 \end{bmatrix} \\ &= \frac{1}{a_2^2 + 2b_2^2} \begin{bmatrix} a_1a_2 + 2b_1b_2 & -a_1b_2 + a_2b_1 \\ -2a_2b_1 + 2a_1b_2 & a_1a_2 + 2b_1b_2 \end{bmatrix} \in K \end{aligned}$$

(9) List all of the generators of the cyclic group $\mathbf{Z}_5 \times \mathbf{Z}_3$.

$([a]_5, [b]_3)$, where $a \in \{1, 2, 3, 4\}$ and $b \in \{1, 2\}$.

(10) Find the order of the element $([9]_{12}, [15]_{18})$ in the group $\mathbf{Z}_{12} \times \mathbf{Z}_{18}$.

Since $o([9]_{12}) = \dfrac{12}{\gcd(9, 12)} = 4$ and $o([15]_{18}) = \dfrac{18}{\gcd(15, 18)} = 6$, $o(([9]_{12}, [15]_{18})) = \mathrm{lcm}[4, 6] = 12$.

(11) Show that if $p > 2$ is a prime, then any group of order $2p$ has an element of order 2 and an element of order $p$.

*Proof.* By Lagrange's theorem, an element can have order $1, 2, p$ or $2p$.

(i) If $G$ has an element of order $2p$, then it is cyclic. It implies that $G \cong \mathbf{Z}_{2p} \cong \mathbf{Z}_2 \times \mathbf{Z}_p$, and so it has an element of order 2 and at least one element (in fact, $p-1$ elements) of order $p$ since $p > 2$ is a prime.

(ii) If $G$ is not cyclic, then the only possible orders of elements are $1, 2$ or $p$. Since $|G|$ is even, it has at least one element of order 2 (see Homework 2 # 12). And it must contain an element of order $p$. (The proof is similar as the proof of Proposition 6 in §3.6.) In particular, suppose that all the non-identity elements have order 2. Then we can always find a subgroup $\{e, a, b, ab\}$ of order 4, which is isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$, since $|G| = 2p > 4$. Thus, we obtain a contradiction since $4 \nmid 2p$, and so it must contain an element of order $p$.

□

(12) Prove that

(a) $\mathbf{Z}_{17}^{\times} \cong \mathbf{Z}_{16}$.

*Proof.* Define $\phi : \mathbf{Z}_{16} \to \mathbf{Z}_{17}^{\times}$ by $\phi([n]_{16}) = [3]_{17}^{n}$. And it is easy to show that $\phi$ is an isomorphism. The motivation for defining such $\phi$ is that $\mathbf{Z}_{16} = \langle [1]_{16} \rangle$ and $\mathbf{Z}_{17}^{\times} = \langle [3]_{17} \rangle$. In particular, there is an easier way to show this isomorphism. We can see that $o([3]_{17}) = 16$ in $\mathbf{Z}_{17}^{\times}$, and so it is cyclic since $|\mathbf{Z}_{17}^{\times}| = 16$. By Theorem 2 (b) in §3.5, we have $\mathbf{Z}_{17}^{\times} \cong \mathbf{Z}_{16}$. To show $o([3]_{17}) = 16$ in $\mathbf{Z}_{17}^{\times}$:

$$[3]_{17}^2 = 9, \quad [3]_{17}^4 = [-4]_{17}, \quad [3]_{17}^8 = [16]_{17} = [-1]_{17}.$$

This is because the order of an element in $\mathbf{Z}_{17}^{\times}$ must be a divisor of 16. □

(b) $\mathbf{Z}_{30} \times \mathbf{Z}_2 \cong \mathbf{Z}_{10} \times \mathbf{Z}_6$.

*Proof.* $\mathbf{Z}_{30} \times \mathbf{Z}_2 \cong \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5 \times \mathbf{Z}_2$ and $\mathbf{Z}_{10} \times \mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_5 \times \mathbf{Z}_2 \times \mathbf{Z}_3$. There is a natural isomorphism between them. □

(13) Is $\mathbf{Z}_{20}^{\times}$ cyclic? Is $\mathbf{Z}_{50}^{\times}$ cyclic?

$\mathbf{Z}_{20}^{\times} = \{\pm 1, \pm 3, \pm 7, \pm 9\}$ is not cyclic since $-1$ and $\pm 9$ have order 2, while $\pm 3$ and $\pm 7$ have order 4. That is, there is no element of order 8.

$\mathbf{Z}_{50}^{\times}$ is cyclic since $o([3]_{50}) = 20 = \varphi(50) = |\mathbf{Z}_{50}^{\times}|$. In particular,

$$[3]_{50}^2 = [9]_{50}, \quad [3]_{50}^4 = [31]_{50}, \quad [3]_{50}^5 = [93] = [-7]_{50}, \quad [3]_{50}^{10} = [49] = [-1]_{50}.$$

Again it is because that $o([3]_{50})$ must be a divisor of $20 : 1, 2, 4, 5, 10, 20$.

(14) (a) In $\mathbf{Z}_{30}$, find the order of the subgroup $\langle [18]_{30} \rangle$; find the order of $\langle [24]_{30} \rangle$.

$\langle [18]_{30} \rangle = \langle [6]_{30} \rangle \Rightarrow$ its order is 5. $\langle [24]_{30} \rangle = \langle [6]_{30} \rangle \Rightarrow$ its order is 5.

(b) In $\mathbf{Z}_{45}$, find all elements of order 15.

$15 = o([k]_{45}) = \dfrac{45}{\gcd(k, 45)} \Rightarrow \gcd(k, 45) = 3 \Rightarrow \gcd(\dfrac{k}{3}, 15) = 1$. Thus, $[k]_{45} =$

$$[3]_{45}, [6]_{45}, [12]_{45}, [21]_{45}, [24]_{45}, [33]_{45}, [39]_{45}, [42]_{45}.$$

(15) Prove that if $G_1$ and $G_2$ are groups of order 7 and 11, respectively, then the direct product $G_1 \times G_2$ is a cyclic group.

*Proof.* $G_1$ and $G_2$ are cyclic since 7 and 11 are primes. Let $o(a) = 7$ in $G_1$ and $o(b) = 11$ in $G_2$. Then $o((a, b)) = \mathrm{lcm}[7, 11] = 77$ in $G_1 \times G_2$. Hence proved. □

(16) Prove that $D_{12} \not\cong D_4 \times \mathbf{Z}_3$.

*Proof.* In $D_{12}$, by Proposition 1 in §3.5, we know that $o(a^k) = \dfrac{12}{\gcd(k, 12)}$. Thus,

| $a^k$ | $e$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $a^7$ | $a^8$ | $a^9$ | $a^{10}$ | $a^{11}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| order | 1 | 12 | 6 | 4 | 3 | 12 | 2 | 12 | 3 | 4 | 6 | 12 |

It follows from Exam II (6) Part (a) that all the remaining elements of the form $a^k b$ have the order 2 since $a^k b \neq e$. In particular, there are only two elements of order 6 in $D_{12}$. However, there are $(5 \cdot 2) = 10$ elements of order 6 in $D_4 \times \mathbf{Z}_3$. Since

- In $D_4$, the possible orders of elements are $1, 2, 4$.
- In $\mathbf{Z}_3$, the possible orders of elements are $1, 3$.

$6 = \text{lcm}[2, 3]$ : Choose $(a, b)$ such that $o(a) = 2$ in $D_4$ and $o(b) = 3$ in $\mathbf{Z}_3$.

- Elements of order 2 in $D_4$ are: $a^2, b, ab, a^2b, a^3b$
- Elements of order 3 in $\mathbf{Z}_3$ are: $[1]_3, [2]_3$

□

(17) For any elements $\sigma, \tau \in S_n$, show that $\sigma\tau\sigma^{-1}\tau^{-1} \in A_n$.

*Proof.* $\sigma$ and $\sigma^{-1}$ have the same number of transpositions in the product. In particular, we write $\sigma = \rho_1\rho_2 \cdots \rho_k$ for $\rho_1, \rho_2, \ldots, \rho_k$ are transpositions. Then $\sigma^{-1} = \rho_k \cdots \rho_2\rho_1$. This also holds for $\tau$. It follows that $\sigma\tau\sigma^{-1}\tau^{-1}$ must have even number of transpositions in the product since the parity of a permutation won't change, i.e., $\sigma\tau\sigma^{-1}\tau^{-1} \in A_n$. □

(18) Find the formulas for all group homomorphisms from $\mathbf{Z}_{18}$ to $\mathbf{Z}_{30}$.

All group homomorphisms from $\mathbf{Z}_{18}$ to $\mathbf{Z}_{30}$ must have the form

$$\phi : \mathbf{Z}_{18} \to \mathbf{Z}_{30} \text{ defined by } \phi([x]_{18}) = [mx]_{30} \text{ for some } [m]_{30} \in \mathbf{Z}_{30}.$$

This $\phi$ is well-defined if and only if $30|18m$. This means that $5|3m$, and so $5|m$ since $\gcd(5, 3) = 1$. Then, all the possible $[m]_{30}$'s are $[0]_{30}, [5]_{30}, [10]_{30}, [15]_{30}, [20]_{30}, [25]_{30}$. Thus, the formulas for all homomorphisms from $\mathbf{Z}_{18}$ into $\mathbf{Z}_{30}$ are:

$$\begin{aligned}
\phi_0([x]_{18}) &= [0]_{30} \\
\phi_5([x]_{18}) &= [5x]_{30} \\
\phi_{10}([x]_{18}) &= [10x]_{30} \\
\phi_{15}([x]_{18}) &= [15x]_{30} \\
\phi_{20}([x]_{18}) &= [20x]_{30} \\
\phi_{25}([x]_{18}) &= [25x]_{30}
\end{aligned}$$

defined for all $[x]_{18} \in \mathbf{Z}_{18}$.

(19) Let $G$ be a group. For $a, b \in G$ we say that $b$ is **conjugate** to $a$, written $b \sim a$, if there exists $g \in G$ such that $b = gag^{-1}$. Following part (a), the equivalence classes of $\sim$ are called the **conjugacy classes** of $G$.

(a) Show that $\sim$ is an equivalence relation on $G$.

*Proof.* (i) Reflexive: $a \sim a$ since $a = eae^{-1}$.

(ii) Symmetric: If $a \sim b$, then $a = gbg^{-1}$ for some $g \in G$, and so $b = g^{-1}a(g^{-1})^{-1}$, which shows that $b \sim a$.

(iii) Transitive: If $a \sim b$ and $b \sim c$, then $a = g_1 b g_1^{-1}$ and $b = g_2 c g_2^{-1}$ for some $g_1, g_2 \in G$. Thus, $a = g_1(g_2 c g_2^{-1})g_1^{-1} = (g_1 g_2)c(g_1 g_2)^{-1}$, and so $a \sim c$.

□

(b) Show that $\phi_g : G \to G$ defined by $\phi_g(x) = gxg^{-1}$ is an isomorphism of $G$.

*Proof.* (i) well-defined: Trivial.

(ii) $\phi_g$ is a homomorphism: For any $x, y \in G$, we have

$$\phi_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = \phi_g(x)\phi_g(y).$$

(iii) $\phi_g$ is onto: For any $x \in G$, we have $\phi_g(g^{-1}xg) = g(g^{-1}xg)g^{-1} = x$.

(iv) $\ker(\phi_g) = \{x \in G \mid \phi_g(x) = gxg^{-1} = e\} = \{x \in G \mid x = g^{-1}eg\} = \{e\}$.

The desired results follow from the fundamental homomorphism theorem. □

(c) Show that a subgroup $N$ of the group $G$ is normal in $G$ if and only if $N$ is a union of conjugacy classes.

*Proof.* $N$ is normal if and only if $gag^{-1} \in N$ for all $a \in N$ and $g \in G$. This implies that $b \in N$ if $b \sim a$, and so $N$ contains the conjugacy class of $a$. It is equivalent to say that $N$ is a union of conjugacy classess since $a$ is an arbitrary element of $N$. This completes the proof. □

(20) (a) List the cosets of $\langle [9]_{16} \rangle$ in $\mathbf{Z}_{16}^{\times}$, and find the order of each coset in $\mathbf{Z}_{16}^{\times}/\langle [9]_{16} \rangle$.

$\mathbf{Z}_{16}^{\times} = \{[1]_{16}, [3]_{16}, [5]_{16}, [7]_{16}, [9]_{16}, [11]_{16}, [13]_{16}, [15]_{16}\}$. Then we have

| coset of $\langle [9]_{16} \rangle$ | order | reason |
|---|---|---|
| $\langle [9]_{16} \rangle = \{[1]_{16}, [9]_{16}\}$ | 1 | trivial |
| $[3]_{16} \cdot \langle [9]_{16} \rangle = \{[3]_{16}, [11]_{16}\}$ | 2 | $[3]_{16}^2 = [9]_{16}$ |
| $[5]_{16} \cdot \langle [9]_{16} \rangle = \{[5]_{16}, [13]_{16}\}$ | 2 | $[5]_{16}^2 = [25]_{16} = [9]_{16}$ |
| $[7]_{16} \cdot \langle [9]_{16} \rangle = \{[7]_{16}, [15]_{16}\}$ | 2 | $[7]_{16}^2 = [49]_{16} = [1]_{16}$ |

(b) List the cosets of $\langle [7]_{16} \rangle$ in $\mathbf{Z}_{16}^{\times}$. Is the factor group $\mathbf{Z}_{16}^{\times}/\langle [7]_{16} \rangle$ cyclic?

| coset of $\langle [7]_{16} \rangle$ | order | reason |
|---|---|---|
| $\langle [7]_{16} \rangle = \{[1]_{16}, [7]_{16}\}$ | 1 | trivial |
| $[3]_{16} \cdot \langle [7]_{16} \rangle = \{[3]_{16}, [5]_{16}\}$ | 4 | $[3]_{16}^2 = [9]_{16}, [3]_{16}^4 = [1]_{16}$ |
| $[9]_{16} \cdot \langle [7]_{16} \rangle = \{[9]_{16}, [15]_{16}\}$ | 2 | $[9]_{16}^2 = [1]_{16}$ |
| $[11]_{16} \cdot \langle [7]_{16} \rangle = \{[11]_{16}, [13]_{16}\}$ | 4 | $[11]_{16}^2 = [9]_{16}, [11]_{16}^4 = [1]_{16}$ |

The factor group is cyclic. In fact, it easily follows from $[3]^2 \notin \langle [7]_{16} \rangle$.

(21) Let $G$ be the dihedral group $D_6$ and let $H$ be the subset $\{e, a^3, b, a^3 b\}$ of $G$.

(a) Show that $H$ is subgroup of $G$.

*Proof.* It is easy to see that $H$ is closed under the multiplication. In particular,

$$ba^3 = a^{-3}b = a^3 b. \quad \text{[See Homework 7 (3)-(a)]}$$

This completes the proof since $H$ is a finite subset. □

(b) Is $H$ a normal subgroup of $G$?

No. Since $aH \neq Ha$. In particular, we have

$$aH = \{a, a^4, ab, a^4b\}, \text{ while } Ha = \{a, a^4, ba = a^5b, a^3ba = a^2b\}.$$

Hence proved.

(22) Let $H$ and $N$ be normal subgroups of a group $G$, with $N \subseteq H$. Define

$$\phi : G/N \to G/H \text{ by } \phi(xN) = xH, \text{ for all cosets } xN \in G/N.$$

(a) Show that $\phi$ is a well-defined onto homomorphism.

*Proof.* (i) well-defined: If $xN = yN$, then $y^{-1}x \in N \subseteq H$, and so $y^{-1}x \in H$. This implies that $xH = yH$, i,e., $\phi(xN) = \phi(yN)$.

(ii) $\phi$ is a homomorphism. For any $xN, yN \in G/N$, we have

$$\phi(xNyN) = \phi(xyN) = xyH = xHyH = \phi(xN)\phi(yN).$$

(iii) $\phi$ is onto: Trivial.

□

(b) Show that $(G/N)/(H/N) \cong G/H$.

*Proof.* $\ker(\phi) = \{xN \in G/N \mid \phi(xN) = xH = H\} = \{xN \in G/N \mid x \in H\}$. This implies that $\ker(\phi)$ is the left cosets of $N$ in $H$, i.e., $\ker(\phi) = H/N$. It follows from the fundamental homomorphism theorem that

$$(G/N)/(H/N) \cong G/H.$$

□

Note that this problem is also called the "Third isomorphism theorem".
Furthermore, HW9 (10) is also called the "Second isomorphism theorem".

---

$* * *$ *The solution is also available on the course website.* $* * *$

---

Review Lecture Slides/Recordings & Homework Assignments

*Good luck for the final* !

---