Algebra comments

Sophie Marques

Thursday 8th October, 2015

Of course this does not cover all the class notes and it is not enough to do the midterm. It is just a way to extract the very important part of the course and I do not mean that you do not have to know the remaining part. THIS ARE NOT ALLOWED FOR THE MIDTERM, IF USED, 0 ON THE MIDTERM WILL BE APPLIED.

What are the essential definitions, properties, results that you need to know?

Equivalence relation

Definition 0.0.1. 1. *If X is a set, a* **relation** *between points in X is defined by specifying some subset R in the Cartesian product $X \times X$. Once R is given, we say that a is related to b indicated by writing $a \sim_R b$ (or simply $a \sim b$) if the pair (a, b) lies in R.*

2. *A relation R in a set X is called an* **RST relation**, *or* **equivalence relation**, *if it has the following properties*

   (a) *$x \sim x$ for all $x \in X$ (the relation is* reflexive*)*

   (b) *$x \sim y \Rightarrow y \sim x$ for all $x, y \in X$ (the relation is* symmetric*)*

   (c) *$x \sim y$ and $y \sim z \Rightarrow x \sim z$ (the relation is* transitive*)*

We say that "x is equivalent to y" if $x \sim_R y$. The **equivalence class** *of a point $x \in X$ is the set $[x]_R = \{y \in X : y \sim_R x\}$.*

Definition 0.0.2. *(Equivalence classes) Let R be an equivalence relation on X. Given a point p in X, we define its* **equivalence class** *to be the set*

$$[p] = \{y \in X : y \sim_R p\}$$

p is called a **representative** *of the equivalence class.*
Since $p \in [p]$, the equivalence classes fill X. Every RST relation corresponds to a partition of the underlying set X into disjoint subsets that fill X.

Lemma 0.0.3. *Let R be an equivalence relation on X. Its equivalence classes have the following properties:*

1. *If $C = [p]$ is an equivalence class and $p' \in [p]$ then $[p'] = [p]$;*
2. *If $C_1 = [p_1]$ and $C_2 = [p_2]$ are two equivalence classes in X, then either $C_1 = C_2$ (the sets are identical) or $C_1 \cap C_2 = \varnothing$ (the sets are disjoint).*

Definition 0.0.4. *(The quotient space X/R) Given a set X and an RST relation R on it, the associated* **quotient space** *X/R is defined to be the set whose elements are the equivalence classes $[x]_R$ in X.*
Be careful! Points in the quotient space X/R are subsets of the original space X. Having defined X/R, there is a natural **quotient map** *$\pi : X \to X/R$ defined by taking*

$$\pi(x) = [x]_R = \text{the equivalence class of } x$$

This map is clearly surjective.

Divisibility

Definition 0.0.5. *Let a and b be integers, $a \neq 0$.*
a divides b *or $a|b$ or* ***b is divisible by a*** *or* ***b is a multiple of a*** *or* ***a is a divisor of b*** *if there exist an integer c such that $b = ca$.*

Theorem 0.0.6. *Let a, b, c, x, y be integers.*

1. *If $a|b$, the $a|xb$.*
2. *If $a|b$ and $a|c$, then $a|bx + cy$.*
3. *If $a|b$ then $xa|xb$.*
4. *If $a|b$, then $|a| \leqslant |b|$. In particular, if $a|b$ and $b|a$, then $a = \pm b$.*

GCD and LCM

Definition 0.0.7. *Let a and b be integers, not both zeros. The* ***greatest common divisor*** *(also called* ***highest common factor****, abbreviated as G. C. D. or H. C. F.) of a and b, denoted as $gcd(a, b)$, is defined to be the largest integer which divides both a and b.*
That is $d = gcd(a, b)$.

1. *$d|a$ and $d|b$;*
2. *$d > 0$;*
3. *For any $d' \in \mathbb{Z}$ such that $d'|a$ and $d'|b$ then $d'|d$.*

Definition 0.0.8. *Let a and b be integers, not both zeros. The* ***lowest common divisor*** *(abbreviated as L. C. M.) of a and b, denoted as $lcm(a, b)$, is defined to be the largest integer which divides both a and b.*
That is $d = lcm(a, b)$.

1. *$a|d$ and $b|d$;*
2. *$d > 0$;*
3. *For any $d' \in \mathbb{Z}$ such that $a|d'$ and $b|d'$ then $d|d'$.*

Prime number

Definition 0.0.9. *We say that an integer $p > 1$ is a **prime integers** if its only divisors are 1 and itself.*
*An integer $n > 1$ which is not prim is said to be **composite**; such an integer integer has the form $n = ab$ where $1 < a < n$ and $1 < b < n$.*

Corollary 0.0.10. *Let a, b, c and m be non-zero integers. Then*

1. $gcd(ma, mb) = |m|gcd(a, b)$.
2. $gcd(a, m) = gcd(b, m) = 1$ *if and only if* $gcd(ab, m) = 1$,
3. $c|ab$ *and* $gcd(b, c) = 1$ *imply* $c|a$,
4. $a|c$, $b|c$ *and* $gcd(a, b) = 1$ *imply* $ab|c$
5. $gcd(a, b) = gcd(b, a) = gcd(a, b + ma)$,
6. $gcd(a, b)lcm(a, b) = |ab|$.

Lemma 0.0.11. *An integer $n > 1$ is composite if and only if it is divisible by some $p \leqslant \sqrt{n}$.*

Euclidean division

Lemma 0.0.12 (Existence and unicity of the Euclidean division)**.** *Let a and b be integers, $a \neq 0$. There exists unique integers q and r such that*

$$a = bq + r$$

with $0 \leqslant r < |a|$.

Euclidean algorithm

Theorem 0.0.13. *Let a and b be positive integers, $a > b$. Then we apply a series of divisions as follows.*

$$\begin{array}{rcll} a & = & bq_0 + r_1 & 0 \leqslant r_1 < b, \\ b & = & r_1q_1 + r_2 & 0 \leqslant r_2 < r_1, \\ r_1 & = & r_2q_2 + r_3 & 0 \leqslant r_3 < r_2, \\ & . & & \\ & . & & \\ & . & & \\ r_{n-2} & = & r_{n-1}q_{n-1} + r_n & 0 < r_n < r_{n-1}, \\ r_{n-1} & = & r_nq_n. & \end{array}$$

The process of division comes to an end when $r_{n+1} = 0$. The integer r_n is the G. C. D. of a and b.

Bezout's identity

Theorem 0.0.14. *Let a and b be integers with $gcd(a, b) = d$. There exist integers u and v such that*

$$au + bv = d.$$

Such u, v can be obtained by backward tracing of the Euclidean divisions in finding the G. C. D, called **Extended GCD algorithm**.

Theorem 0.0.15. *Let a and b be integers (not both 0) with greatest common divisor d. Then, an integer c has the form $ax + by$ for some x, $y \in \mathbb{Z}$ if and only if c is a multiple of d. In particular, d is the least positive integer of the form $ax + by$ $(x, y \in \mathbb{Z})$.*

Corollary 0.0.16. *Two integers a and b are coprime if and only if there exist integers x and y such the*

$$ax + by = 1.$$

The fundamental theorem of arithmetic

Lemma 0.0.17. *Let p be a prime, and let a and b any integers. Then either p divides a, or a and p are coprime;*

Lemma 0.0.18 (Gauss lemma)**.** *Let p be a prime, and let a and b any integers. Then p divides ab if and only if p divides a or p divides b.*

Theorem 0.0.19 (Fundamental theorem of arithmetic)**.** *Each integer $n > 1$ has a prime-power factorization*

$$n = p_1^{e_1}...p_k^{e_k}$$

where $p_1, \ldots, p_k$ are distinct primes and $e_1, \ldots, e_k$ are positive integers; this factorization is unique, apart from permutations of the factors.

Remarque 0.0.20. *The prime-power factorizations allows us to calculate products, quotients, powers, greatest common divisors and least common multiples. Suppose that integers a and b have factorizations*

$$a = p_1^{e_1}...p_k^{e_k} \text{ and } b = p_1^{f_1}...p_k^{f_k}$$

(where we have $e_i, f_i \geqslant 0$ to allow for the possibility that some prime p_i may divide one but not both of a and b). Then we have

$$\begin{array}{rcl} ab & = & p_1^{e_1+f_1}...p_k^{e_k+f_k}, \\ a/b & = & p_1^{e_1-f_1}...p_k^{e_k-f_k} \ (if\ b|a), \\ a^m & = & p_1^{me_1}...p_k^{me_k}, \\ gcd(a,b) & = & p_1^{min(e_1,f_1)}...p_k^{min(e_k,f_k)} \\ lcm(a,b) & = & p_1^{max(e_1,f_1)}...p_k^{max(e_k,f_k)} \end{array}$$

where $min(e,f)$ and $max(e,f)$ are the minimum and maximum of e and f.

Units U_n.

Definition 0.0.21. *An element $[a] \in \mathbb{Z}/n\mathbb{Z}$ has a* ***multiplicative inverse*** *if there exists some $[k] \in \mathbb{Z}/n\mathbb{Z}$ such that $[k] \cdot [a] = [a] \cdot [k] = [1]$. If it exists this inverse or "reciprocal" is denoted by $[a]^{-1}$. The invertible elements in $\mathbb{Z}/n\mathbb{Z}$ are the* ***units*** *of the system $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$; we denote them by U_n.*

Theorem 0.0.22. *If $n > 1$, the group of units in $\mathbb{Z}/n\mathbb{Z}$ is*

$$U_n = \{[k] \in \mathbb{Z}/n\mathbb{Z} : 1 \leqslant k \leqslant n - 1 \text{ and } gcd(k, n) = 1\}$$

Corollary 0.0.23. *If $n > 1$ is an integer then all elements $[a] \neq [0]$ in $\mathbb{Z}/n\mathbb{Z}$ have multiplicative inverses $\Leftrightarrow$ the modulus n is a prime. This means $\mathbb{Z}/p\mathbb{Z}$ is a* **field** *for each prime $p > 1$, in which division is allowed by taking*

$$[a]/[b] = [a][b]^{-1}$$

for all pairs such that $[b] \neq [0]$.

Group theory.

Definition 0.0.24. *A* **group** *is a set G equipped with a binary operation mapping $G \times G \to G$. Such a "product operation" carries each ordered pair (x, y) in the Cartesian product set $G \times G$ to a group element which we write as $x \cdot y$ or simply xy. The product operation is required to have the following properties.*

G.1 **Associativity:** $(xy)z = x(yz)$, *for all* $x, y, z \in G$.
This insures that we can make sense of a product $x_1 \ldots x_n$ involving several group elements without inserting parentheses to indicate how elements are to be combined two at a time. However, the order in which elements appear in a product is crucial! While it is true that $x(yz) = xyz = (xy)z$, the product xyz can differ from xzy.

G.2 **Unit element:** *There exists an element $e \in G$ such that $ex = x = xe$, for all $x \in G$. (One can prove that e is unique)*

G.3 **Inverses exist:** *For each $x \in G$ there exists an element $x^{-1} \in G$ such that $xx^{-1} = e = x^{-1}x$. (One can prove that x^{-1} is unique)*
The inverse element x^{-1} is called the **multiplicative inverse** *of x.*
The group G is said to be **commutative** *or* **abelian** *if the additional axiom.*

G.4 **Commutativity:** $xy = yx$, *for all* $x, y \in G$ *is satisfied.*

We write $|G|$ for the number of elements in G, which could be ∞.

Get use to the additive notation. Here is a glossary for translating between multiplicative and additive notation:

	Identity	*Inverse*	*Product*	*Powers*
Multiplicative notation $(G, \cdot)$	e	x^{-1}	$x \cdot y$	$x^k = x \ldots x$
Additive notation $(G, +)$	0	$-x$	$x + y$	$k \cdot x = x + \cdots + x$

Definition 0.0.25. *A non-empty subset H in a group G is a* **subgroup** *(we denote $H \leqslant G$) if it has the properties*

1. *H is closed under formation of products: $H \cdot H \subseteq H$, or equivalently $x, y \in H \Rightarrow xy \in H$;*
2. *The identity element e lies in H.*

3. H is closed under inverses: $h \in H \Rightarrow h^{-1} \in H$.

The trivial groups $H = (e)$ and $H = G$ are subgroups; all other subgroups, if any, are referred to as **proper subgroups**

Characteristic subgroup of a group, (they help to understand better a group).

Definition 0.0.26. *1. The* **center** *$Z(G)$ of a group G is the set of elements that commute with everyone in G*

$$Z(G) = \{x \in G : gx = xg \text{ for all } g \in G\}$$

These elements form a subgroup that is one of the most important structural features of any group. An element $g \in G$ is in the center $Z(G)$ if and only $gxg^{-1} = x$ for all x, so we may write

$$Z(G) = \{g : gxg^{-1} = x \text{ for all } x \in G\}$$

Obviously G is abelian $\Leftrightarrow Z(G) = G$.

More generally, given a nonempty subset $S \subseteq G$ we may define

2. The **centralizer** *of S is $Z_G(S) = \{x \in G : xs = sx \text{ for all } s \in S\}$ Notice that x is in the centralizer if and only if $xsx^{-1} = s$ for each $s \in S$. That is a stronger requirement than the condition $xSx^{-1} = S$ mentioned next, which would allow points to be moved around within S as long as the set S remains invariant.*

3. The **normalizer** *of S is $N_G(S) = \{x \in G : xSx^{-1} = S\}$ Both $Z_G(S)$ and $N_G(S)$ are subgroups of G, with $N_G(S) \supseteq Z_G(S) \supseteq Z(G)$.*

Characterization of finite groups

Theorem 0.0.27. *Let H be a nonempty* FINITE *subset of a group G, such that $H \cdot H = \{h_1h_2 : h_1, h_2 \in H\}$ is equal to H. Then the identity element e automatically lies in H and H is a subgroup of G.*

Homomorphism, (they permits to compare groups, understand better complicated group thanks to simpler group)

Definition 0.0.28. *1. A* **homomorphism** *between two groups* $(G, \cdot)$ *and* $(G', *)$ *is any map* $\phi : G \to G'$ *that* **intertwines** *the group operations, in the sense that*

$$\phi(x \cdot y) = \phi(x) * \phi(y) \qquad \textit{for all } x, y \in G \tag{1}$$

(One can prove that $\phi(e) = e'$ *and* $\phi(x^{-1}) = (\phi(x)^{-1})$*.)*

2. The map is an **isomorphism** *if it is a homomorphism and is also a bijection. Then the inverse map* $\phi^{-1} : G' \to G$ *exists and it is also a homomorphism.*

When you have an isomorphism between two group, you can think of them as perfectly the same as GROUP (you are just changing the name of the elements).

Definition 0.0.29. *Certain terminology is standard in discussing homomorphisms* $\phi : G \to G'$ *of groups.*

1. *The* **kernel** *of* ϕ *is the set of elements that get "killed" by* ϕ*:*

$$\ker(\phi) = \{x \in G : \phi(x) = e'\} \quad ,$$

where e' *is the identity element in* G'*. The kernel is a subgroup of the initial group* G*.*

2. *The* **range** $\mathrm{range}(\phi)$ *is the forward image of the initial group*

$$\mathrm{range}(\phi) = \phi(G) = \{\phi(x) : x \in G\}$$

The range is always a subgroup of the target group G'*, but it may be a proper subgroup.*

Knowing the range and the kernel is important when studying an homomorphism.
VERY IMPORTANT TO KEEP IN MIND.

Lemma 0.0.30. *A homomorphism* $\phi : G \to G'$ *is one-to-one* $\Leftrightarrow$ $\ker(\phi) = (e)$

Generated subgroup

Definition 0.0.31. *Let S be a nonempty subset of a group G. The intersection*

$$< S >= \cap\{H : H \text{ is a subgroup and } S \subseteq H\}$$

is a subgroup. It is called the **subgroup generated by** *S, and the elements of S are referred to as "generators" of this group.*

Definition 0.0.32. *Subgroups generated by a single element are called* **cyclic subgroups**.

Theorem 0.0.33 (The exponent laws)**.** *Let $(G, \cdot)$ be a group. For any element $a \in G$ and any $k \in \mathbb{N}$ define*
— $a^k = a \cdot \dots \cdot a$ *(k times);*
— $a^0 = e$ *(the identity element);*
— $a^{-k} = (a^{-1}) \cdot \dots \cdot (a^{-1})$ *(k times).*
Then the following **exponent laws** *are valid for all $m, n \in \mathbb{Z}$.*

1. $a^m \cdot a^n = a^{m+n}$;

2. $(a^m)^{-1} = (a^{-1})^m$;

3. $(a^m)^n = a^{mn}$.

If G is abelian we also have

4. *If G is abelian we also have* $(ab)^n = a^n \cdot b^n$.

Definition 0.0.34. *Let $(G, \cdot)$ be a group. The* **order** *$o(a)$ of a group element $a \in G$ is the smallest positive exponent $k > 0$ such that $a^k = e$. If no such exponent exists the group element is said to have* **infinite order**, *which we indicate by writing $o(a) = \infty$.*

VERY IMPORTANT THEOREM

Theorem 0.0.35 ((Structure of Cyclic Subgroups).)**.** *Let $(G, \cdot)$ be a group. A cyclic subgroup has the form $H = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ for some $a \in G$. There are two possibilities, which depend on the order $o(a)$ of the generator.*

(a) $o(a) = \infty$. *Then all powers a^k, $k \in \mathbb{Z}$, are distinct and $H \simeq (\mathbb{Z}, +)$ embedded in the abstract group G.*

(b) $o(a) = k < \infty$. *Then $H = \{e, a, a^2, \ldots, a^{k-1}\}$, with $a^k = e$. In this case $H \simeq (\mathbb{Z}/k\mathbb{Z}, +)$ embedded in the abstract group G.*

Proposition 0.0.36. *Every subgroup of a cyclic group is also cyclic.*

Theorem 0.0.37. *For $n > 1$, a nonzero element $x = [k]$ in $\mathbb{Z}/n\mathbb{Z}$ is a cyclic generator under the $(+)$ operation $\Leftrightarrow \gcd(k, n) = 1$ – i.e. if and only if $[k]$ lies in the set U_n of multiplicative units in $\mathbb{Z}/n\mathbb{Z}$.*

Cosets

Definition 0.0.38. *Given any subgroup $H \subseteq G$, its* **left cosets** *are the subsets of the form $xH = \{xh : h \in H\}$ with $x \in G$. These are of interest because the whole group splits into a disjoint union of its distinct cosets xH. One can also define* **right cosets** *as sets of the form Hx, right translates of H by elements $x \in G$. There is no difference between left- and right cosets if the group G is abelian. The group element x is a* **coset representative** *for xH.*

Lemma 0.0.39. *Let H be a subgroup in G and let x, y be points in G. Then*

(a) *We have $xH = yH \Leftrightarrow$ there is some $h \in H$ such that $y = xh$. In particular, $xH = H \Leftrightarrow x \in H$.*

(b) *Two cosets xH and yH are either identical sets in G or are disjoint. The cosets form a partition of G.*

(c) *The relation $x \underset{R}{\sim} y \Leftrightarrow xH = yH$ is reflexive, symmetric, and transitive, and the equivalence classes for this relation are precisely the cosets in G/H: for any x the class $[x] = \{g \in G : g \underset{R}{\sim} x\}$ is equal to xH.*

(Good to understand, and keep in mind:

Proposition 0.0.40. *If $\phi : G \to G'$ is a homomorphism of groups and $K = \ker(\phi)$ is its kernel, then*

(a) *All points in a coset xK map to a single point in G' under ϕ. Thus a homomorphism is constant on each coset of its kernel.*

(b) *Distinct cosets $xK \neq yK$ in G are disjoint, with $xK \cap yK = \emptyset$, and they map to* DISTINCT *points in G'.*

Furthermore ϕ is one-to-one, and hence an ISOMORPHISM *from G to the subgroup $\text{range}(\phi) \subseteq G'$, if and only if its kernel is trivial: $\ker(\phi) = (e)$.*
)

Quotient

Definition 0.0.41. *The* **space of cosets** G/H *is just the quotient space of equivalence classes under the* RST *relation* $x \underset{R}{\sim} y$. *Note carefully:*

> *Points in the quotient space* G/H *are subsets in the original group* G.

The **quotient map** $\pi : G \to G/H$ *for this relation is given by*

$$\pi(x) = xH \qquad \textit{(since } xH \textit{ is the equivalence class for } x\textit{)}$$

General properties of this **surjective map** *follow directly from this definition.*

- *Under* π, *each coset* $xH \subseteq G$ *collapses to a single point in the quotient space* G/H.
- *Distinct (disjoint) cosets* $xH \neq yH$ *in* G *are mapped by* π *to distinct points in the quotient space* G/H.

REMEMBER, that G/H is NOT necessarily a group, if no condition on H or G are added!

Normal subgroup

NORMALITY is a necessary and sufficient condition to make G/H into a group. That is the motivation of defining normal subgroup!

Definition 0.0.42. *A subgroup N in G is a* **normal subgroup** *if it has the property*

$$xN = Nx \qquad \text{for all } x \in G \ , \tag{2}$$

which means there is no difference between left- and right-cosets of N. All subgroups are normal if G is abelian. Normality of a subgroup is indicated by writing $N \lhd G$. □

Lemma 0.0.43. *If N is a subgroup of G, each condition below implies the others.*

(a) *The subgroup N is normal: $xN = Nx$ for all $x \in G$.*

(b) *$xNx^{-1} = N$ for all $x \in G$.*

(c) *$xNx^{-1} \subseteq N$ for all $x \in G$.*

(d) *$xnx^{-1} \in N$ for all $x \in G, n \in N$.*

Here a nice characterization of normal subgroup:

Lemma 0.0.44. *A subgroup N in a group G is normal if and only if N is the kernel $\ker\phi = \{x \in G : \phi(x) = e'\}$ for some homomorphism $\phi : G \to G'$.*

NORMAL subgroup define QUOTIENT GROUP:

Theorem 0.0.45 (Quotient groups)**.** *Let N be a* NORMAL *subgroup in a group G. Then the operation*

$$(xN) \odot (yN) = xyN \qquad \text{for } x, y \in G \ . \tag{3}$$

is well defined: the outcome does not depend on the particular coset representatives x and y. This product satisfies all the group axioms, making the coset space G/N into a group in its own right. Finally, the quotient map $\pi : G \to G/N$ becomes a surjective homomorphism of groups with $\ker(\pi) = N$.

Isomorphism theorem

VERY IMPORTANT THEOREM

Theorem 0.0.46 (First Isomorphism Theorem)**.** *Let $\phi : G \to G'$ be a homomorphism, let $K = \text{ker}(\phi)$, and let $\pi : G \to G/K$ be the quotient homomorphism. There is a unique map $\tilde{\phi} : G/K \to R = \text{range}(\phi)$ that makes the diagram*

$$\begin{tikzcd}
G \arrow[r, "\phi"] \arrow[d, "\pi"'] & R \subseteq G' \\
G/K \arrow[ur, "\tilde{\phi}"'] &
\end{tikzcd}$$

commute: $\tilde{\phi} \circ \pi = \phi$. This map is a group homomorphism and is bijective, so it is an isomorphism from the quotient group G/K to $R = \text{range}(\phi)$. In particular, when ϕ is surjective we have $G' \cong G/K$.

(LESS USED FOR YOU but still good to know:

Theorem 0.0.47 (Second Isomorphism Theorem)**.** *Let A be any subgroup in G and let N be a normal subgroup. Then*

(a) The product set AN is a subgroup in G, with $N \lhd AN$.

(b) $A \cap N$ is a normal subgroup in A.

(c) $AN/N \cong A/(A \cap N)$

Hint: In (c) consider the map $\psi : A/(A \cap N) \to AN/N$ given by $\psi(a(A \cap N)) = aN$ for $a \in A$. Start by showing this map is well-defined: if $a(A \cap N) = a'(A \cap N)$ then $aN = a'N$ □

Theorem 0.0.48 (Third Isomorphism Theorem)**.** *Let $G \supseteq A \supseteq B$ be groups such that A and B are both normal subgroups in G. Prove that $(G/B)/(A/B) \cong G/A$.*
Note: This is the group-theory analog of the arithmetic relation $(a/c)/(b/c) = a/b$.

)

LAGRANGE theorem

VERY IMPORTANT THEOREM!

Theorem 0.0.49 ((Lagrange))**.** *If G is a group of finite order $|G| = n$ and H is a subgroup, then $|H|$ must divide $|G|$. In fact, we have*

$$|G| = |G/H| \cdot |H| \tag{4}$$

so the number of left cosets in G/H also divides $|G|$.

(You should know how to prove all these immediate corollary).

Corollary 0.0.50. *If G is a finite group and $a \in G$ then the order $o(a)$ of this element must divide $|G|$.*

Corollary 0.0.51. *If a group G has finite order $|G| = n$ then $a^n = e$ for all elements $a \in G$.*

Corollary 0.0.52. *If G is a finite group whose order is a prime $|G| = p > 1$, then $G = \langle a \rangle$ for every element $a \neq e$ and $G \cong (\mathbb{Z}/p\mathbb{Z}, +)$. In particular, every finite group of prime order is cyclic, abelian.*

Theorem 0.0.53. *In $(\mathbb{Z}/n\mathbb{Z}, +)$, for every divisor d of n, $(1 \leqslant d \leqslant n)$ there is a* UNIQUE *(cyclic) subgroup $H_d (=< [n/d] >)$ such that $|H_d| = d$*

Exercises ”TYPE” that you MUST really know how to solve in order to solve the basic part of the midterm.

Of course, it is up to changing the values involved. Of course, more abstract exercises will be asked, and I cannot put all into an exercise ”TYPE”. All this exercises are direct applications of the notes.

1. Prove using induction on n that 4 divides $1 + 3^{2n+1}$ for all $n \in N$. Do not forget that there is 3 step to follow:

   (a) Initialization, $n = 1$ (depending of where you have to start!)

   (b) Transmission: State induction hypothesis, that is:
   Suppose that the statement is true for SOME ARBITRARY n, and PROVE that the statement is true for n+1 (Be careful! DO NOT forget to use the induction hypothesis).

   (c) Conclusion: By induction, the statement is true for all $n \in \mathbb{N}$.

2. Compute $gcd(24, 36)$. (You might want to use or the extended GCD algorithm, or prime factorization, or direct computation. Depending on how big are the numbers involved.)

3. Compute $lcm(24, 36)$. (You might want to use prime factorization, or direct computation. Depending on how big are the numbers involved.)

4. Prove that 12 and 35 are coprime. (Note that this is the same question as asking: is the fraction 12/35 irreducible, for example) You may use GCD extended algorithm to find that gcd is equal to 1, or direct computation, but also Bezout's theorem (useful when the number are not fixed: remember the exercise of the homework 1: Let $a \in \mathbb{Z}$. Prove that $gcd(2a + 3, a + 2) = 1$ or the one on the class note: Prove that the fraction $(21n + 4)/(14n + 3)$ is irreducible for every natural number n.)

5. Compute the Euclidean division of 100 by 13. (Here I ask you to find the quotient and the remainder) That is $100 = 13 \times 7 + 9$ (i.e. $q = 7$, $r = 9$).

6. Find an integer solution (or I can ask all the congruence classes solutions mod the GCD of)

$$gcd(2445, 652) = 2445 \times x + 652 \times y$$

(You might use the extended GCD algorithm to do so).

7. Compute the inverse of $[2]$ in U_3. (to compute the multiplicative inverse of a unit $[k]$ in $\mathbb{Z}/n\mathbb{Z}$: find integers r, s such that $rk + sn = 1$ (whose existence is guaranteed if $gcd = 1$). Then $rk \equiv 1 \ (mod \ n)$ and $[k]^{-1} = [r]$. The extended GCD algorithm is a fast algorithm for computing such a pair r, s.)

8. Compute U_12. (For this just use the fact that

$$U_{12} = \{[k] : gcd(k, 12) = 1, 0 \leqslant k \leqslant 11\}$$

9. When I ask you that something satisfies a definition. Let's say, Prove

   (a) That a relation is an equivalence relation;

   (b) That a set is a group, subgroup, normal subgroup;

   (c) That a map is a homomorphism

   First right down the definition as you know it from the class (in a draft), then retranslate it apply to the particular example given in the exercise (make sure you understand well how the relation is defined and what is fixed what is not, or for a group, subgroup

   (a) what is the operation? Am I in additive or multiplicative notation?

   (b) what should be the identity element? (and prove it)

   (c) what should the inverse ? (and prove it)

   or for a morphism: what are the two operation for each group (be careful they might be different!)

   and then rewrite in the draft what you need to prove for this particular relation, this particular group, this particular subgroup, this particular normal subgroup (if the exercise does not tell you that a normal subgroup is a subgroup, you need to prove it before proving the normality of the subgroup!)

10. If I ask you to prove that a morphism is injective, COMPUTE the kernel and prove that it is trivial. That's it. To do so, write the definition of the kernel as you remember in a draft, then apply it to you particular example (you need for this to know what is your morphism and what is the identity element of the target group, then try to find out by rewriting it as much as you can why it is trivial!) (Apply this method for computing a center, centralizer, normalizer).
11. if I ask you to prove that a map is surjective, find a pre image for any element of the target. And, if I ask if a map is an isomorphism, prove that is surjective and injective or find an explicit inverse and prove that it is an inverse.
12. If you define a map from a quotient space, do not forget to first of all prove that it is well defined that your definition does not depend on the choice that you make of the representative.
13. To prove that a subgroup H of a group G is generated by some given elements of G, you need to prove
    (a) that these element are in H, and
    (b) that if you choose another arbitrary subgroup H' of G containing these element then it must contain H (since H by definition is the smallest subgroup of G containing these element).
    (c) Do not forget you know the structure of any cyclic group!
    (d) If you have to prove that a quotient G/H is isomorphic to another group G', you might want to use the isomorphism theorem, that is create a canonical (natural) morphism from $G \to G'$ whose kernel is H which is surjective.
    (e) Do not forget Lagrange theorem when question asked about order.

Advice to overcome the level of abstraction of this class.

Practice!

The only way to do math is to practice as well as to do sport. Did you ever see a athlete being good just by learning about the theory of the sport he want to be good at ? I have never. For the exact same reason, you will never do math just know the theory, the muscle you are stimulating is your brain. So my main advice is to do all the examples, proofs, homework of the class by your self (even more than once). You might need first to be helped by the answer I gave with. But, at some point, you have to be able to pick an exercise/example without the solution, sit without anything else and do it in a quick amount of time. So, also, take time to do your homework seriously, it is better to do half perfectly and understood than all completely badly and in a rush. At some point, you need to write a proof with your own words. If you are lost, mimic the examples of the class notes for a start and when you get it, you will be wanting to try it without the solution.

Overcome the step one by one!

Here, the step that you need to overcome one by one, (you cannot miss a step) in order to do mathematics:

1. Know how to apply result, compute (for example what you do in calculus)
2. Understand new concepts
3. Understand the proof of the result that you know how to apply or example given in class.
4. Be able to reconstruct a proof, example, that you have seem, using logic knowing the main ideas of it.
5. Construct a proof to answer to an exercises using ideas that arise from the proof, examples that have been given to you in class.
6. Make your proof as concise and precise as possible and take the quicker rout to answer the question. The quicker rout does not mean using a very strong theorem to prove a trivial statement. If you use a theorem in some sense you use also its proof and then your proof is long if the proof of what you want to prove will be long as well. The length of your proof depends on the length of the theorem you use.
7. Create new concept, new conjecture, new techniques, new mathematics (this is for researchers).

I am here to give you a panel of idea that you can use, then it is you who need to practice to be able to understand when they can be used and will permit you to reach the answer. It is not easy and it takes time.

Change your expectation!

I do not know what you except of a teacher. I think if you except that everything at the end of the course seems easy and clear and that you have to do nothing at home to understand, in my opinion, it is not the right thing to except. And if I did this, I will make you robots that are only able to reproduce a single one thing. I think I would be lying to you to tell you that mathematics is very easy. As any other discipline it takes practice. The main point of my work I guess is to make you able to work in perfect autonomy and leave some liberty to your mind to think maybe in something that I have even not think about. You cannot manage in math by learning by heart. Maybe you have to change your expectation toward what a mathematical class should bring you, other than the concepts, I introduce to your that you could find in any book any notes I could write, and you could read by yourself at home, you need to acquire mathematical intuition that you cannot learn in the book. In order to make you understand this I need you to know the concept from the previous class, then I could stimulate your intuition and logic, in class. If you do not have the tools, we cannot work. If you really want to success and be always up to date, just take a while to review the concept right before the class even just for 30 min, you might progress fast. Hopefully it might help you a lot. Everyone is different of course and for some of you everything might be fluid but for most of you, you might win a lot in doing just this.

Methodology! Learn to do a proof!

One thing that I noticed and that you know by now, is that most of you even the best of you have to learn how to organize, write a proof. It is important for any discipline that you learn how to express your idea in a coherent, concise, comprehensible way. You need to learn how to do an induction, a proof by contraposition, a simple direct proof, a proof by contrapositive. But, beside this, how to make yourself perfectly clear.
A general proof steps:

1. Sometimes you might want to work on the different equivalent way that you can retranslate the question, the hypotheses might help you to choose which part of the course will permit you to answer the question, until reaching the point that you get an idea that works and solve the problem QUICKLY (the most important step that you acquire with practice). Here you are almost done if you know how to be clear and organize, and if you have some methodology. Sometimes it is all about writing down a general definition in the context of the exercise, using the appropriated notations.
2. Organize your idea, see if everything is there (all the hypotheses needed) to apply your ideas, sometimes retranslate the theorem, definition that you want to use in the particular case of the exercise.
3. Write down your proof. I want to see, connectors as: We suppose ...., If ..., Then ..., As a consequence, ..., And ...., Or.....,Since..., As .. In order to make your proof smooth and fluid (as a line, that is not broken). But I want also to see what results you are using when you are using it and why you can use it, if you are using a theorem that you have not proven in the line before. Should look like something as: "Since we have $a \not\equiv 0 \ mod \ p$, we can use Fermat's little theorem this give us : .... blablabla.... ", for instance.
4. Reread your proof afterword, please. (While practicing, compare your proof with the notes or ask a friend if he understands it or just leave it alone one day and comeback to it and try to understand yourself after).

Again, you can see a proof as an algorithm that you put into a computer which knows your class material, and is able to reach it only if you tell him what you are using and you have all the hypothesis needed to apply the theorem. Of course, you need to tell him the connexion between them because as everyone knows a computer is stupid. If the computer does not get stuck until the end, and you reach the conclusion. You have a correct proof. If not something is missing. Then you have to make sure that the algorithm is as short as possible keeping in mind that when you call a theorem you need to pass on the computer all its proof. This is a hard thing to do. For now just manage to solve the problem correctly with a right proof in any case you will loose point by itself, penalize yourself, if you use a too long proof during the exam, because you will be loosing time.

During the MIDTERM! Breath, keep calm, THINK and Sometimes be lazy choosing the shorter exit to the solution!

1. **THINK**, do not write down the solution to fast, avoid traps, **THINK!**, but don't be too slow!
2. Take time to read each questions until the end (it might give you ideas on how to solve it) and if needed transform it in an equivalent way that can be more convenient to use.
3. Do not forget to use every hypothesis if they are there there is a reason, tell me when you use each hypothesis to make sure you are not missing one and because it will justify why you are doing what you are doing. Also, if you are missing one most probably your proof has a problem.
4. Think about all the material that you can use related to the question. And try to find the most efficient way to solve it. Having the right idea is the main part of your work, then it is easier.
5. Try to put idea together in a logical way without missing step, in order to finally, write a mathematical proof. DO NOT forget the logical connector (as: if, then, suppose, As a consequence, this is equivalent, if and only if, and, or.............) and make sure they are the right ones to use.
6. If you need to prove that something satisfies a definition you can first write the definition applied to your particular example and then prove each points of the definition. It might be easier to write it down in a draft.
7. Make sure you answered the initial question in the end. Sometimes one looses point just because they stop just before finishing.
8. Reread what you wrote sometimes it is a big mess that even not you I am sure, could even understand. How could I ?
9. Keep in mind that the Midterm that you handle to me it is not a **DRAFT**. I do not want statement all over the pages without logical

connexion between then, like a puzzle that I have to assemble, that will not work at all.

10. Do not write long paragraph trying to convince me that you know how to do, PROVE IT and I will be convince. A proof is a succession of true mathematical statement linked with logical connector. If you are writing a paragraph as you could right it in a english class or literature that is not a proof, you trying to convincing yourself and at the same time me that your ”argument” work. Also, a drawing is not a proof, could be part of your draft to help you to think.
11. If it takes plenty of computations and pages to reach the solution, please ask your self isn’t it a clever way in order to solve the problem? Using the class notes ?