Name———————————————, ID ————————

MTH 532 Abstract Algebra 2020, 1–121

MTH532-Course Portfolio-Spring 2020

Ayman Badawi

Table of contents

1 Section 1: (No change)Course Syllabus

A	Course Title & Number	**ABSTRACT ALGEBRA: MTH 532**
B	Pre/Co-requisite(s)	Admission to MSMTH program
C	Number of credits	3
D	Faculty Name	Ayman Badawi
E	Term/ Year	Spring 2020
F	Sections	

CRN	Course	Days	Time	Location
	MTH 532	S	12—14:45	Nab 007

G Instructor Information

Instructor	Office	Telephone	Email
Ayman Badawi	NAB 262	XXX	I prefer: abadawi@aus.edu

Office Hours: By appointment

H Course Description from Catalog

Covers basic properties of groups, normal subgroups and direct sum of groups; homomorphism and isomorphism between groups; classification of finite abelian groups; and applications of Sylow's Theorems. Introduces rings, ideals, polynomial rings, irreducible and prime elements of rings, unique factorization domains, fields and their extensions including finite fields.

I Course Learning Outcomes

Upon completion of the course, students will be able to:

- Develop mathematical proofs and reason abstractly in exploring properties of rings and groups. (Exam I, Exam II, and Final)
- Demonstrate an understanding of Lagrange Theorem and its applications, symmetric groups, quotient groups, cyclic groups. (Exam I and Final)
- Demonstrate an understanding of the structure of finite abelian groups (Exam I and Final).
- Demonstrate an understanding of Sylow's Theorems and their applications (Exam I and Final)
- Demonstrate an understanding of the intellectual structure of rings, ideals, prime ideals, primary ideals, 2-absorbing ideals, maximal ideals, prime elements, irreducible elements and quotient rings. (Exam II and Final)
- Use and apply homomorphism and isomorphism theory between rings and groups. (Exam I, Exam II and Final)
- Demonstrate an understanding of fields, and field extension (Exam II and Final)

	• Demonstrate an understanding of separable fields, splitting fields, Galois field, finite fields, and cyclotomic field extension. (Exam II and Final)
J Textbook and other Instructional Material and Resources	Primary: Instructor class notes. I-Learn, my personal webpage http://ayman-badawi.com/MTH%20530.html and http://ayman-badawi.com/MTH%20531.html Reference: David S. Dummit and Richard M. Foote, *Abstract Algebra*- Third Edition Any graduate textbook will do.
K Teaching and Learning Methodologies	The teaching and learning tools used in this course to deliver the subject matter include white board and markers, formal lectures, class discussions, assignments, two exams and a final
L Grading Scale, Grading Distribution, and Due Dates	**Grading Scale** A:85—100, A- : 81--84.99 , B+: 77--- 80.99, B: 74 -- 76.99, B-: 70 – 73.99 , C+: 67 --- 69.99, C: 63—66.99 , F <63

Excellent	
A	Equals 4.00 grade points
Meet Expectation	
A-	Equals 3.80 grade points
B+	Equals 3.30 grade points
B	Equals 3.00 grade points
Below Expectation	
B-	Equals 2.70 grade points
C+	Equals 2.30 grade point
C	Equals 2.00 grade point
Fail	
F	Equals 0.00 grade points
Academic Integrity Violation Fail	

XF	Equals 0.00 grade points
Withdrawal Fail	
WF	Equals 0.00 grade points

Grading Distribution

Assessment	**Weight**	**Date**
Homework	15 %	
Mid-Term one	25 %	
Mid-Term two	25%	
Final Exam	35%	Comprehensive
Total	100 %	

M	**Explanation of Assessments**	Exams, homework assignments will include proofs. So students are expected to master some of the techniques that are commonly used in Abstract Algebra
N	**Student Academic Integrity Code Statement**	Student must adhere to the Academic Integrity code stated in the graduate catalog.

SCHEDULE

*Note: **Tests and other graded assignments due dates are set.** No addendum, make-up exams, or extra assignments to improve grades will be given.*

#	WEEKS	CHAPTER/SECTIONS	NOTES
	1--6	**Groups, subgroups, cyclic groups, symmetric groups, quotient groups, product of groups, normal subgroups, Sylow's groups, classification of finite abelian groups, group homomorphism and isomorphism** **EXAM I**	Definitions, Examples, proofs
	7-13	**Rings, ideals, prime ideals, primary ideals, 2-absorbing ideals, maximal ideals, quotient rings, quotient fields, prime elements, irreducible elements, product of rings, localized rings, fields**	Definition Examples Proofs

		Exam II	
	14--16	**separable fields, splitting fields, cyclotomic fields, finite fields, and Galois field**	

2 Section 2: Instructor Teaching Material

2.1 HANDOUTS

2.1.1 Handout on the Unit-Group of Z_n

Name————————————————, ID ——————————

U(n) is cyclic? , MTH 532, Spring 2020

Ayman Badawi

$n \geq 3$**. Then** $U(n)$ **is cyclic iff** $n = 4$**,** $n = p^m$**, or** $n = 2p^m$ **for some odd prime** p **and integer** $m \geq 1$**.**

Suppose that $n = 4$ or $n = p^m$, or $n = 2p^m$ for some odd prime p and integer $m \geq 1$. We show that $U(n)$ is cyclic.

If $n = 4$, $U(4) \approx Z_2$ is cyclic. If $n = p^m$ for some odd prime p and integer $m \geq 1$, then $\phi(n) = (p-1)p^{m-1}$. Hence $U(n) \approx z_{p-1} \oplus z_{p^{m-1}}$. Since $gcd(p-1, p^{m-1}) = 1$, $U(n)$ is cyclic. If $n = 2p^m$ for some odd prime p and integer $m \geq 1$, then $\phi(n) = (p-1)p^{m-1}$. Hence $U(n) \approx z_{p-1} \oplus z_{p^{m-1}}$. Since $gcd(p-1, p^{m-1}) = 1$, $U(n)$ is cyclic.

Now assume that $n \neq 4$ and $n \neq p^m$, and $n = 2p^m$ for some odd prime p and integer $m \geq 1$. We show that $U(n)$ is not cyclic.

Case 1. Asuume $n = 2^m$, $m \geq 3$. Then $U(n) \approx z_2 \oplus z_{2^{m-2}}$. Since $gcd(2, 2^{m-2}) \neq 1$, $U(n)$ is not cyclic.

Case 2. Assume $n = 2^k p^m$, p is odd prime, $k \geq 2$, and $m \geq 1$. Then $\phi(n) = 2^{m-1}(p-1)p^{m-1}$. Thus $U(n) \approx D = z_2 \oplus z_{2^{m-2}} \oplus z_{p-1} \oplus z_{p^{m-1}}$. Now $H = z_2 \oplus \{0\} \oplus z_{p-1} \oplus \{0\}$ is a subgroup of D. Since $gcd(2, p-1) \neq 1$, H is not a cyclic subgroup of D. Thus D is not not cyclic (we know every subgroup of a cyclic group is cyclic). Hence $U(n)$ is not cyclic.

Case 3. Assume $n = 2p_1^{k_1} p_2^{k2} \cdots p_m^{k_m}$, where $m \geq 2$, $p_1, ..., p_m$ distinct prime odd integers. Then $\phi(n) = (p_1 - 1)p^{k_1 - 1}(p_2 - 1)p_2^{k_2 - 1} .... (p_m - 1)p_m^{k_m - 1}$. Thus $U(n) \approx D = z_{(p_1 - 1)} \oplus z_{p^{k_1 - 1}} \oplus z_{(p_2 - 1)} \oplus z_{p_2^{k_2 - 1}} \oplus .... \oplus z_{(p_m - 1)} \oplus z_{p_m^{k_m - 1}}$ (note $m \geq 2$). Now $H = z_{p_1 - 1} \oplus \{0\} \oplus z_{p_2 - 1} \oplus \{0\} \oplus ... \oplus \{0\}$ is a subgroup of D. Since $gcd(p_1 - 1, p_2 - 1) \neq 1$, H is not a cyclic subgroup of D. Thus D is not not cyclic. Hence $U(n)$ is not cyclic.

Case 4. Assume $n = 2^k p_1^{k_1} p_2^{k2} \cdots p_m^{k_m}$, where $m \geq 2$ and $k \geq 2$, $p_1, ..., p_m$ distinct prime odd integers. Then $\phi(n) = 2^{m-1}(p_1 - 1)p^{k_1 - 1}(p_2 - 1)p_2^{k_2 - 1} .... (p_m - 1)p_m^{k_m - 1}$. Thus $U(n) \approx D = z_2 \oplus z_{2^{m-2}} \oplus z_{(p_1 - 1)} \oplus z_{p^{k_1 - 1}} \oplus z_{(p_2 - 1)} \oplus z_{p_2^{k_2 - 1}} \oplus .... \oplus z_{(p_m - 1)} \oplus z_{p_m^{k_m - 1}}$ (note $m, k \geq 2$). Now $H = \{0\} \oplus \{0\} \oplus z_{p_1 - 1} \oplus \{0\} \oplus z_{p_2 - 1} \oplus \{0\} \oplus ... \oplus \{0\}$ is a subgroup of D. Since $gcd(p_1 - 1, p_2 - 1) \neq 1$, H is not a cyclic subgroup of D. Thus D is not not cyclic. Hence $U(n)$ is not cyclic.

Case 5. Assume n is odd. Then $n = p_1^{k_1} p_2^{k2} \cdots p_m^{k_m}$, where $m \geq 2$, $p_1, ..., p_m$ distinct prime odd integers. Then $\phi(n) = (p_1 - 1)p^{k_1 - 1}(p_2 - 1)p_2^{k_2 - 1} .... (p_m - 1)p_m^{k_m - 1}$. Thus $U(n) \approx D = z_{(p_1 - 1)} \oplus z_{p^{k_1 - 1}} \oplus z_{(p_2 - 1)} \oplus z_{p_2^{k_2 - 1}} \oplus .... \oplus z_{(p_m - 1)} \oplus z_{p_m^{k_m - 1}}$ (note $m \geq 2$). Now $H = z_{p_1 - 1} \oplus \{0\} \oplus z_{p_2 - 1} \oplus \{0\} \oplus ... \oplus \{0\}$ is a subgroup of D. Since $gcd(p_1 - 1, p_2 - 1) \neq 1$, H is not a cyclic subgroup of D. Thus D is not not cyclic. Hence $U(n)$ is not cyclic.

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: `abadawi@aus.edu`, `www.ayman-badawi.com`

2.1.2 Handout on Rings

Name————————————, ID ——————

Useful Information for Second Exam, Final, Common Knowledge , MTH 532, Spring 2020

Ayman Badawi

Fact 1. Let A be a commutative ring with 1 and $f(X) \in A[X]$. Then $f(X) \in Nil(A[X])$ if and only if the coefficients of $f(X)$ are nilpotent elements of A.

Example: $f(X) = 3X^3 + 6X^2 + 12X + 24$ is a nilpotent element of the polynomial ring $Z_{27}[X]$ (i.e., $f(X) \in Nil(Z_{27}[X])$, i.e., there exists a positive integer n such that $f(X)^n = 0$ in $Z_{27}[X]$ since the coefficients of $f(x)$ are nilpotent elements of Z_{27}. (note that $3, 6, 12, 24 \in Nil(Z_{27})$)

Example : $f(X) = 5X^3 + 2x + 4$ is not a nilpotent element of $Z_8[X]$ since $5 \notin Nil(Z_8)$.

Fact 2. Let A be a commutative ring with 1 and $f(X) = a_nX^n + \cdots + a_1X + a_0 \in A[X]$. Then $f(X) \in U(A[X])$ if and only if $a_n, ..., a_1 \in Nil(A)$ and $a_0 \in U(A)$.

Example: $f(X) = 3X^3 + 6X^2 + 12X + 7$ is a unit (invertible) element of the polynomial ring $Z_{27}[X]$ (i.e., $f(X) \in U(Z_{27}[X])$, i.e., there exists a polynomial $k(X) \in Z_{27}[X]$ such that $f(X)k(X) = 1$ in $Z_{27}[X]$ since 3, 6, 12 are nilpotent elements of Z_{27} and the constant term $a_0 = 7 \in U(Z_{27})$.

Example : $f(X) = 2X^3 + 5X + 4$ is not a unit (invertible) element of $Z_8[X]$ since $5 \notin Nil(Z_8)$ and the constant term $a_0 = 4 \notin U(Z_8)$.

Example : $f(X) = 2X^3 + 5X + 3$ is not a unit (invertible) element of $Z_8[X]$ since $5 \notin Nil(Z_8)$.

Fact 3. (**Surprising result!**) Let A be a commutative ring with 1 and $f(X) = a_nX^n + \cdots + a_1X + a_0 \in A[X]$. Then $f(X) \in Z(A[X])$ if and only if $a_n, ..., a_1 \in Z(A)$ and $bf(X) = 0$ for some nonzero $b \in Z(A)$.

Example: $f(X) = 3X^3 + 2X^2 + 3X + 2$ is not a zero-divisor element of the polynomial ring $Z_6[X]$ (i.e., $f(X) \notin Z(Z_6[X])$, i.e., there is no nonzero-polynomial $k(X) \in Z(Z_6[X]$ such that $f(X)k(X) = 0$ in $Z_6[X]$. Why? because $Z(Z_6) = \{0, 2, 3\}$, but $bf(X) \neq 0$ for every nonzero $b \in Z(Z_6)$.

Example : $f(X) = 10X^3 + 20X + 10$ is a zero-divisor element of the polynomial ring $Z_{30}[X]$ (i.e., $f(X) \in Z(Z_{30}[X])$, i.e., there is a nonzero-polynomial $k(X) \in Z(Z_{30}[X]$ such that $f(X)k(X) = 0$ in $Z_{30}[X]$. Why? because $3 \in Z(Z_{30})$ and $3f(X) = 0$.

Fact 4. Let A be a commutative ring with 1. Then $Nil(A)$ is a proper ideal of A.

Trivial: Let $a, b \in Nil(A)$. Then $a^n = b^m = 0$ for some positive integers n, m. Hence by EXPANSION, we have $(a - b)^{n+m} = 0$ Thus $a - b \in Nil(A)$. Also, $(ab)^m = a^mb^m = a^m.0 = 0$. Hence $ab \in Nil(A)$. Thus $Nil(A)$ is a subring of A. Now let $f \in A$. Then $(fa)^n = f^na^n = f^n.0 = 0$. Hence $fa \in Nil(A)$. Thus $Nil(A)$ is a proper ideal of A (note $Nil(R) \cap U(A) = \emptyset$).

Fact 5. (**Nice result on how to find nilpotent elements in** Z_n). Write $n = p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$ (of course $p_1, ..., p_k$ are distinct prime integers) and let $m = p_1p_2\cdots p_k$. Then $Nil(Z_n) = (m) = mZ_n = span\{m\}$ is the ideal of Z_n generated by $m \in Z_n$.

Example: Let $A = Z_{75}$. Then $n = 75 = 3.5^2$ and $m = 3.5 = 15$. Hence $Nil(A) = (15) = 15A = span\{15\} = \{0, 15, 30, 45, 60\}$.

Example : Let $A = Z_{30}$. Then $n = 30 = 2.3.5$ and $m = 2.3.5 = 0 \in Z_{30}$. Hence $Nil(A) = (0) = 0A = span\{0\} = \{0\}$.

Fact 6. (**Recall (from lecture) this is nice result on how to find prime ideals and maximal ideal in** Z_n). Write $n = p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$ (of course $p_1, ..., p_k$ are distinct prime integers). Let $A = Z_n$. Then a proper ideal I of A is a prime ideal of A if and only I is a maximal ideal of A if and only if $I = (p_i) = p_iA$ for some $1 \leq i \leq k$.

Example: Let $A = Z_{75}$. Then $n = 75 = 3.5^2$. Hence $3A = \{0, 3, 6, 9, 12, ..., 72\}$ and $5A = \{0, 5, 10, ..., 70\}$ are the only prime (maximal) ideals of A.

Example : Let $A = Z_{30}$. Then $n = 30 = 2.3.5$. Hence $2A = \{0, 2, 4, 6, 12, ..., 28\}$, $3A = \{0, 3, 6, ..., 27\}$, and $5A = \{0, 5, 10, ..., 25\}$ are the only prime (maximal) ideals of A.

Fact 7. (**Recall (from lecture) this is a nice result, it is called the Chinese remainder Theorem**): Let A be a commutative ring with 1 and $I_1, I_2, ..., I_k$ are proper ideals of A that are relatively prime ideals of A (i.e., $I_i + I_j = A$ for every $i \neq j$, $1 \leq i, j \leq k$, some authors call such ideals co-prime ideals). Let $F = I_1 \cap I_2 \cap \cdots \cap I_k$. Then A/F is ring-isomorphic to $A/I_1 \oplus A/I_2 \oplus \cdots \oplus A/I_k$. In particular, if $F = \{0\}$, then A is ring-isomorphic to $A/I_1 \oplus A/I_2 \oplus \cdots \oplus A/I_k$.

Fact 8. (**Nice result, make sure that you know it**): Let B, C be commutative rings with 1 and $A = B \oplus C$. Let F be a proper ideal of A. Then $F = I_1 \oplus I_2$ for some ideal I_1 of B and some ideal I_2 of C. Furthermore (nice), A/F is ring-isomorphic to $B/I_1 \oplus C/I_2$. Furthermore (from Lecture):

(a) F is a prime ideal of A if and only if either $F = I \oplus C$ for some prime ideal I of B or $F = B \oplus J$ for some prime ideal J of C.

(b) F is a maximal ideal of A if and only if either $F = I \oplus C$ for some maximal ideal I of B or $F = B \oplus J$ for some maximal ideal J of C.

Fact 9. Let A be a commutative ring with 1 and I be a proper ideals of A. Then I is a prime ideal of A if and only if $A - I$ is a multiplicative subset of A (recall from lecture that what I call multiplicative subset of A, some authors call it multiplicatively closed subset of A). The proof is so trivial (just use definitions)

REMARKS Let A be a commutative ring with 1.
(a) Note that every subring of A is a multiplicative subset of A.
(b) Note that every subgroup of $U(A)$ is a multiplicative subset of A
(c) Chose an element $a \in A$. Then $D = \{a, a^2, a^3, ..., a^n, ...\} = \{a^m \mid m$ is a positive integer $\}$ is a multiplicative subset of A.
d) an ideal I of A is proper if and only if $1 \notin$ [Easy: Suppose I is an ideal and $1 \notin I$. We claim that I is proper. Deny. Hence $I \cap U(A) \neq \emptyset$. Suppose there is a unit (invertible) element $u \in I$. Since I is an ideal of A and $u^{-1} \in A$, we have $1 = u^{-1}u \in I$, a contradiction.
e) A proper ideal of I of Z is prime if and only if I is a maximal ideal of Z if and only if $I = pZ = (p)$ for some prime integer p of Z. Thus the prime ideals of Z are maximal ideals of Z and they are of the form pZ for some prime integer p. (Proof is trivial : We know that the proper ideals of Z has the form nZ for some positive integer n. Now assume that nZ is a prime ideal of Z. Hence Z/nZ is an integral domain. But Z/nZ is Z_n. Thus Z_n is a finite integral domain and hence a field. Thus n must be a prime number and nZ must be a maximal ideal.
f) A commutative ring A with 1 is called Noetherian if every proper ideal of R is finitely generated., i.e. if I is a proper ideal of A, then $I = span\{a_1, ..., a_n\}$ over A for some elements $a_1, ..., a_n \in I$, i.e., if $x \in I$, then there are $b_1, ..., b_n \in A$ such that $x = b_1a_1 + ... + b_na_n$. Interesting result about Noetherian rings : If A is Noetherian, then $A[x_1, ..., x_n]$ is Noetherian (i.e., the polynomial ring with n variables is Noetherian)
g) Let A be a commutative ring with 1. Then the radical of A (denoted by $Rad(A)$) = Intersection of ALL prime ideals of A. It is Known, that the RADICAL of A = Nil(A). (the proof relies on the fact that I proved in the class if I is a proper ideal of A and S is a multiplicative system such that $I \cap S = \emptyset$ then there is a prime ideal P of A such that $I \subseteq P$ and $P \cap S = \emptyset$
h). Let A be a commutative ring with 1. Jacobson radical of A (denoted by $J(A)$) is the intersection of all MAXIMAL ideals of A. Nice result about the Jacobson Radical of A : For every $x \in J(A)$, $x + u \in U(A)$ for every $u \in U(A)$. Also $Rad(A) \subseteq J(A)$ **Faculty information**

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: `abadawi@aus.edu, www.ayman-badawi.com`

2.1.3 Handout on Fields

Useful Information about FIELDS and Galois Extension, Common Knowledge , MTH 532, Spring 2020

Ayman Badawi

1 Q, fields of characteristic 0

QUESTION 1. Assume that $[Q(\alpha) : Q] = n$ and $f(x) \in Q[x]$ is a monic polynomial of degree n such that $f(\alpha) = 0$. Prove that $f(x)$ is an irreducible polynomial over Q. In fact, prove that $f(x) = Irr(\alpha, Q)$.

Solution: Let $k(x) = Irr(\alpha, Q)$. Since $[Q(\alpha) : Q] = n$, we know that $deg(k(x)) = n$ (note that $k(x)$ is the unique monic irreducible polynomial over Q such that $k(\alpha) = 0$). Since $f(\alpha) = 0$, we know (class notes) that $k(x)|f(x)$. Since $f(x)$ and $k(x)$ are monic and $deg(f(x)) = deg(k(x)) = n$, we conclude that $k(x) = f(x)$.

QUESTION 2. Let $\alpha = e^{\frac{2\pi i}{10}}$ and $E = Q(\alpha))$.

(i) Find $[E : Q]$

Solution: By last lecture, note that E is the 10th cyclotomic extension field of Q (i.e, E is the splitting field of the polynomial $x^{10} - 1$, i.e. INSIDE E, we have $x^{10} - 1 = (x - \alpha)(x - \alpha^2)....(x - \alpha^n)$. By class notes, we know $[E : Q] = \phi(10) = 4$.

(ii) What are the roots of $Irr(\alpha, Q)$? Then find $Irr(\alpha, Q)$ written in the general form.

Solution: Let $k(x) = Irr(\alpha, Q)$. Then $deg(k(x)) = \phi(10) = 4$ and by class notes (last lecture), the roots of $k(x)$ are the α^k's, where $gcd(k, n) = 1$, $1 \le k < 10$. Hence the roots are $a_1 = \alpha$, $a_2 = \alpha^3$, $a_3 = \alpha^7$ and $a_4 = \alpha^9$. Hence $k(x) = (x - a_1)(x - a_2)(x - a_3)(x - a_4)$. Now how to find $k(x)$ written in the general form (note $deg(k) = 4$).

Note that $x^{10} - 1 = (x^5 - 1)(x^5 + 1)$. Let $h(x) = x^5 + 1$. Then it is clear that $h(\alpha) = \alpha^5 + 1 = [e^{\frac{2\pi i}{10}}]^5 + 1 = e^{\pi i} + 1 = -1 + 1 = 0$. Thus we know $k(x)|h(x)$. Now observe, we know $x^5 + 1 = (x + 1)(x^4 - x^3 + x^2 - x + 1)$. Let $d(x) = x^4 - x^3 + x^2 - x + 1$. Then $h(x) = x^5 + 1 = (x + 1)d(x)$. Since $h(\alpha) = 0$, we conclude that $d(\alpha) = 0$.

Since $deg(d(x)) = deg(k(x)) = 4$ and $d(\alpha) = k(\alpha) = 0$, by Question 1 we conclude that $k(x) = d(x) = x^4 - x^3 + x^2 - x + 1$.

(iii) Find a basis, B, for E over Q. Then Write $w = \alpha^7 + 4\alpha^6 + 7\alpha^5$ in terms of the elements in the basis B.

Solution: Since $[E : Q] = 4$, by class notes we know $B = \{1, \alpha, \alpha^2, \alpha^3\}$ is a basis of E over Q, i.e., if $b \in E$, then $b = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$ for some $a_0, ..., a_3 \in Q$.

Now remember from the lecture, how we got the basis B: Let $k(x) = Irr(\alpha, Q)$ as in (ii). Then $k(x) = x^4 - x^3 + x^2 - x + 1$ and $M = (k(x))$ is a maximal ideal of $Q[X]$ and $L = Q[x]/M$ is a field. Then by mapping $x + M \to \alpha$, we concluded that L is field-isomorphic to E. Since $\{1 + M, x + M, x^2 + M, x^3 + M\}$ is a basis for L over Q and $x + M \to \alpha$, we conclude that $B = \{1, \alpha, \alpha^2, \alpha^3\}$ is a basis of E over Q. Hence if $a \in L$, then we know that $a = a_0 + a_1x + a_2x^2 + a_3x^3 + M$ and thus $a = a_0 + a_1x + a_2x^2 + a_3x^3 + M$ in L $\leftrightarrow$ $b = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$ in E. Hence $w = \alpha^7 + 4\alpha^6 + 7\alpha^5$ in E $\leftrightarrow$ $x^7 + 4x^6 + 7x^5 + M$ in L. But we know how to find $x^7 + 4x^6 + 7x^5 + M$ in L. Recall we divide $x^7 + 4x^6 + 7x^5$ by $k(x) = x^4 - x^3 + x^2 - x + 1$ (high school math (division a polynomial by another polynomial)) and you find the remainder $r(x)$. I did the calculation, I got $r(x) = -4x - 7$ (if I made a mistake, then just correct it, I do not need to know about it!). Hence $x^7 + 4x^6 + 7x^5 + M = -4x - 7 + M$ in L. Hence $w = \alpha^7 + 4\alpha^6 + 7\alpha^5 = -4\alpha - 7$ in E (if this is not beautiful, then nothing is beautiful!). (see the below Question...to see more beauty)

(iv) Let $a \in E$. Find all possibilities of $deg(Irr(a, Q))$.

Solution: From class notes $deg(Irr(a, Q))$ is a factor of $[E : Q]$. Why? Let $a \in E$. Then $Q(a)$ is a field between Q and E. Hence $[E : Q] = [E : Q(a)][Q(a) : Q]$ and we know that $[Q(a) : Q] = deg(Irr(a, Q))$. Thus $deg(Irr(a, Q))$ is a factor of 4 (since $[E : Q] = 4$). Thus deg(Irr(a, Q)) = 1 or deg(Irr(a, Q)) = 2 or deg(Irr(a, Q)) = 4. Note that if deg((Irr(a, Q)) = 1, then $a \in Q$ and $Irr(a, Q) = x - a$.

(v) Is E a Galois extension field of Q?

Solution: Yes. Why? because $[E : Q]$ is a finite number. Since E is the splitting field of $x^{10} - 1$ (in particular, E is the splitting field of $k(x) = Irr(\alpha, Q) = x^4 - x^3 + x^2 - x + 1$), then E is a normal EXTENSION of Q (remember that E is a normal extension of Q means that for each $a \in E$, $Irr(a, Q)$ has all its roots inside E, i.e., $Irr(a, Q) = (x - a_1)(x - a_2)...(x - a_k)$ for some k that is a factor of 4 (note that we just proved that if $a \not\in Q$), then $Irr(a, Q)$ has degree 2 or 4 and thus it has 2 distinct roots or 4 distinct roots).

(vi) Find all elements of the Galois group $Aut(E/Q)$. How many subgroups does $Aut(E/Q)$ have? Find them all.

Solution: Since E is a Galois extension of Q, we know that $|Aut(E/Q)| = [E : Q] = 4$. Since E is the 10th cyclotomic extension of Q, by class notes we know that $Aut(E/Q)$ is group-isomorphic to $U(10)$. Thus

$|Aut(E/Q)| = [E : Q] = |U(10)| = \phi(10) = 4$. Now let $f \in Aut(E/Q)$. Then $f : E \to E$ is a field isomorphism such that $f(c) = c$ for every $c \in Q$ (i.e., f is one to one, f is onto, f(a + b) = f(a) + f(b) and f(ab) = f(a)f(b)).

To construct these function, observe that if $a \in E$ is a root of $Irr(a, Q)$, then $f(a)$ must be a root of Irr(a, Q) (Why? because f is an isomorphism from E to E). Since each each element in E is a linear combination of 1, α, α^2,α^3, we conclude that f can be determined completely if we know what $f(\alpha)$ maps to . For example if $f(\alpha) = b$, then $f(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3) = a_0 + a_1b + a_2b^2 + a_3b^3$. Now what are the choices of $f(\alpha)$? Since f is an isomorphism from E to E, $f(\alpha)$ must be a root of $Irr(\alpha, Q) = k(x) = x^4 - x^3 + x^2 - x + 1$. Now we know what to do: From part II, the roots of of $k(x)$ are $\alpha, \alpha^3, \alpha^7, \alpha^9$.

Thus here are all elements of $Aut(E/Q)$: $f_1 : E \to E$ such that $f(\alpha) = \alpha$ (identity map), $f_2 : E \to E$ such that $f_2(\alpha) = \alpha^3$, $f_3 : E \to E$ such that $f_3(\alpha) = \alpha^5$, and $f_4 : E \to E$ such that $f_4(\alpha) = \alpha^9$. If you want, you can write $\alpha^5, \alpha^7, \alpha^9$ as linear combination of $1, \alpha, \alpha^2$, and α^3 (as I did in part III, for example $\alpha^5 = -1$), but here we do not need to. Now since $|Aut(E/Q)| = |U(8)| = 4$ and U(10) is cyclic (Why? see class notes, 10 = (2)(5)), we know that the group $Aut(E/Q)$ is isomorphic to Z_4. Let us calculate the order of each element in Aut(E/Q). $|f_1| = 1$ (note f_1 is the identity map). $|f_2| = 4$. Why? note that $Aut(E/Q)$ is a group under composition. Hence we need to find the smallest integer m such that $f_2^m = f_2 \ o \ f_2 o ... \ o \ f_2(mtimes) = f_1$. But here f_2 is determined by $f_2(\alpha) = \alpha^3$. Thus we need to find m such that $[f_2(\alpha)]^m = \alpha$. Now $[f_2(\alpha)]^2 = f_2(f_2(\alpha)) = f_2(\alpha^3) = [f_2(\alpha)]^3 = (\alpha^3)^3 = \alpha^9 \neq \alpha$. Since $|f_2| \neq 2$ and $|f_2|$ must be a factor of 4 (lagrange Theorem), we conclude that $|f_2| = 4$. Important observation, in general, if $f(a) = c^k$ and the operation is composition, then $[f(a)]^m = (f \ o \ o ... \ o f)(\alpha)(mtimes) = c^{k^m}$. So, to see that $[f_2(\alpha)]^4 = \alpha$ (the identity map), $[f_2(\alpha)]^4 = \alpha^{3^4} = \alpha^{81}$. From class notes, observe that the set of all roots of the polynomial $x^{10} - 1$ under normal multiplication is a cyclic group and α generates such groups, i.e., $|\alpha| = 10$. Hence $\alpha^{81} = \alpha^{80}\alpha$ and since $\alpha^{10} = 1$, we conclude $\alpha^{80} = 1$. Thus $\alpha^{81} = \alpha$.

Hence we have Exactly one subgroup of order 1, $G_1 = \{f_1\}$, we have EXACTLY one subgroup of order 2, $G_2 = \{f_1, f_4\}$ (note that $[f_4(\alpha)]^2 = \alpha^{9^2} = \alpha^{81} = \alpha$), and exactly one subgroup of order 4, $G_3 = Aut(E/Q) = \{f_1, f_2, f_3, f_4\} =< f_2 >$.

(vii) Find all distinct fields between Q and E (including Q, and E). For each subfield L between Q and E find $[L : Q]$.

Solution: By last lecture, Galois Theorem tell us that number of all fields between Q and E (including Q and E) is exactly the number of all subgroups of $Aut(E/Q)$ (including the identity map, and $Aut(E/Q)$). From Part VI, Aut(E/Q) has exactly 3 subgroups. Hence there are exactly 3 fields between Q and E (including Q and E). Hence there is exactly one field L between Q and E such that $L \neq Q$ and $L \neq E$. So how to find L. Recall from last lecture, Galois Theorem tell us that each subgroup of Aut(E/Q) fix one and only one field between Q and E. What do we mean with "fix one and only one field between Q and E? here is the meaning (read it CAREFULLY): If G is a subgroup of Aut(E/Q), then there is a largest field , say L, between Q and E such that for every (read carefully for every) $f \in G$, we have $f(i) = i$ for every $i \in L$ and $|G| = |Aut(E/L)| = [E : L]$.

So from part 1. Q is the fixed field that corresponds to the group $G_3 = Aut(E/Q) = \{f_1, f_2, f_3, f_4\}$. E is the fixed field that corresponds to the group $G_1 = \{f_1\} = Aut(E/E)$. Now we need to find a field L that is fixed by $G_2 = \{f_1, f_4\}$, i.e, we need to find the largest field L between Q and E such that for every $i \in L$, we have $f_1(i) = i$ and $f_4(i) = i$. Note that in our case, $L = Q(v)$ for some $v \in E - Q$. So how to find v. Here is a technique that work, here $f_1(\alpha) = \alpha$ and $f_4(\alpha) = \alpha^9$. Take $v = \alpha + \alpha^9$. Check that $v \notin Q$. HOW can I CHECK? write α^9 in terms of 1, α, α^2, and α^3 as I did in part iii. My calculation, showed that $\alpha + \alpha^9 \notin Q$. OBSERVE that $a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0 \in Q$ for some $a_3, ..., a_0 \in Q$ if and only if $a_0 \in Q$, $a_3 = a_2 = a_1 = 0$. For if $a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0 = a_4 \in Q$, then consider the polynomial $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 - a_4$. Then $f(\alpha) = 0$. Hence we know that $k(x) = x^4 - x^3 + x^2 - x + 1 = Irr(\alpha, Q)$ must divide $f(x)$, impossible since $deg(k) = 4$ and $deg(f) \leq 3$. So let $v = \alpha + \alpha^9$. Then $f_1(v) = v$ and $f_4(v) = f_4(\alpha + \alpha^9) = f_4(\alpha) + f_4(\alpha^9) = \alpha^9 + f_4(\alpha)^9 = \alpha^9 + (\alpha^9)^9 = \alpha^9 + \alpha^{81} = \alpha^9 + \alpha = v$ (since $\alpha^{80} = 1$). Thus G_2 fixed the field $Q(v)$. We know by Galois Theorem that $|G_2| = [E : Q(v)]$. Since $|G_2| = 2$, we have $[E : Q(v)] = 2$. To find $[Q(v) : Q]$. We know $[E : Q] = [E : Q(v)][Q(v) : Q]$. Since $[E : Q] = 4$ and $[E : Q(v)] = 2$, we conclude that $[Q(v) : Q] = 2$. Thus note that $Irr(v, Q)$ is a monic irreducible polynomial of degree 2 over Q.

Fact 1. Assume that E is a Galois extension of Q and L is a field between Q and E. If L is not a normal extension of Q, then the group $Aut(E/Q)$ is not abelian group! (waw waw !)

QUESTION 3. Let E be a splitting field of $f(x) = x^7 - 12$, by class notes $E = Q(a_1, ..., a_7)$ where $a_1, ..., a_7$ are the roots of $f(x)$. Show that $Aut(E/Q)$ is a non-abelian group.

Solution: We know every splitting field of a polynomial over Q is a Galois extension of Q. By Einstein result, let $p = 3$, then $p| - 12$ and $3^2 = 9 \nmid -12$. Thus $f(x)$ is IRREDUCIBLE. Clearly $a = \sqrt[7]{12}$ is a root of $f(x)$. Thus $L = Q(a)$ is a field between Q and E and $[L : Q] = 7$. Clearly, $B = \{1, a, a^2, ..., a^6\}$ is a basis of L over Q. Hence all elements in L are real numbers and $i \notin L$. Since $f(x)$ has roots that are not real, $f(x)$ does not SPLIT completely inside L. Hence L is not a normal extension of Q. Thus by the FACT, $Aut(E/Q)$ is not abelian.

QUESTION 4. Let $E = Q(\sqrt{2}, \sqrt[3]{2})$. Find $[E : Q]$. Prove that E is not a Galois extension of Q. Let $a \in E - Q$. Find all possibilities of $degree(Irr(a, Q))$.

Solution: This is how you view E. Let $L = Q(\sqrt{2})$, and $H = Q(\sqrt[3]{2})$. Then $E = L(\sqrt[3]{2}) = H(\sqrt{2})$.

Now, it is clear that $Irr(\sqrt[3]{2}, Q) = x^3 - 2$ and $Irr(\sqrt{2}, Q) = x^2 - 2$. Now $x^3 - 2$ has no roots in L. Thus $x^3 - 2$ stays irreducible over L, i.e., $Irr(\sqrt[3]{2}, L) = x^3 - 2$ (note that $Irr(\sqrt[3]{2}, L) = f(x)$ is the unique irreducible polynomial with coefficient from L such that $f(\sqrt[3]{2}) = 0$). Thus $[E = L(\sqrt[3]{2}) : L = Q(\sqrt{2})] = 3$. It is clear that $[L = Q(\sqrt{2}) : Q] = 2$. Hence $[E : Q] = [E = L(\sqrt[3]{2}) : L][L = Q(\sqrt{2}) : Q] = (3)(2) = 6$.

Also note that $[E : Q] = [E : H][H : Q] = (2)(3) = 6$. We show that E over Q is not a normal Extension, and hence E is not a Galois Extension of Q. Choose $a = \sqrt[3]{2}$. Then $a \in E$. $Irr(a, Q) = x^3 - 2$. Since all elements of E are real numbers and $x^3 - 2$ has 2 non-real roots, $x^3 - 2$ doest not SPLIT over E (i.e., $x^3 - 2$ cannot completely factored as product of linear factors over E, i.e, $x^3 - 2$ does not have all its roots inside E). Hence E over Q is not a normal Extension, and thus E is not a Galois extension of Q.

Now let $a \in E - Q$. Then we know $deg(Irr(a, Q))$ must be a factor of $[E : Q] = 6$. Thus all possibilities of $degree(Irr(a, Q))$ are 2, 3, 6.

Fact 2 (**NICE!**). Def: $F \subseteq E$ (of course F and E are fields) and $E = F(b)$ for some $b \in E$. Then we say E is a simple extension of F. Let $E = Q(a_1, a_2, ..., a_k)$ such that $[E : Q] < \infty$. Then there exist $b \in E$ such that $E = Q(b)$. So, in general if E is a field extension of Q and $[E : Q]$ is finite number, then $E = Q(b)$ for some $b \in E$, i.e., E is a simple extension of Q.

QUESTION 5. Let E be the field in Question 4, i.e., $E = Q(\sqrt{2}, \sqrt[3]{2})$. By the fact above find $b \in E$ such that $E = Q(b)$. Then find $Irr(b, Q)$.

Solution: You will like this technique!. Here is the idea, recall from basic linear algebra. If K is a subspace of V and dim(V) = dim(K), then $K = V$. Claim: $b = \sqrt{2} + \sqrt[3]{2}$. We show $E = Q(b)$. Since $b \in E$, $Q(b)$ is a subspace of E. If we show that $[Q(b) : Q] = 6 = [E : Q]$, then $E = Q(b)$. Here is the Technique! we find $f(x) = Irr(b, Q)$ by "back ward" method.

Set (*)

$$x = \sqrt{2} + \sqrt[3]{2}$$

Use minimum calculations on $(*)$ in order to eliminate all radical. Then we get a polynomial with coefficients in Q. This polynomial will be $Irr(b, Q)$. ONE WAY :

$$x - \sqrt{2} = \sqrt[3]{2}$$

$$(x - \sqrt{2})^3 = 2$$

$$x^3 - 3\sqrt{2}x^2 + 6x - \sqrt{8} = 2$$

Now move all radicals to the right side

$$x^3 + 6x - 2 = 3\sqrt{2}x^2 + \sqrt{8}$$

.

$$(x^3 + 6x - 2)^2 = (3\sqrt{2}x^2 + \sqrt{8})^2 = 18x^4 + 24x^2 + 8$$

Thus all radicals are eliminated. Now we move the right side to the left, then we get our $f(x) = Irr(b, Q)$ of degree 6 such that $f(b) = 0$.

$$Irr(b, Q) = f(x) = (x^3 + 6x - 2)^2 - 18x^4 - 24x^2 - 8 \in Q[x]$$

.

If you want you can simplify $f(x)$ but here there is no need. It is clear that $deg(f) = 6$ and $f(b) = 0$. Thus $[Q(b) : Q] = 6$.

Since $[E : Q] = [Q(b) : Q] = 6$ and $Q(b)$ "lives" inside E, we conclude that $E = Q(b)$.

QUESTION 6. Let $a = \sqrt{3}$ and $b = \sqrt{7}$ and $E = Q(a, b)$. Show that $Q(a, b)$ is a Galois extension of Q. Find all subgroups of $Aut(E/Q)$. For each subgroup H of $Aut(E/Q)$, find the field that is fixed by H.

Solution: Recall from last lecture if $E = Q(a_1, a_2, .., a_k)$ such that for every i, $1 \le i \le k$, $Irr(a_i, Q)$ has all its roots in E (i.e., $Irr(a_i, Q)$ splits in E), then E is a Galois extension of Q. Clearly, $f_a(x) = Irr(a, Q) = x^2 - 3$ and $f_b(x) = Irr(b, Q) = x^2 - 7$. Both polynomials split in E. Thus E is a Galois extension of Q. By similar argument as in Question 4, $[E : Q] = 4$. Hence $Aut(E/Q)$ is a group with 4 elements. We know that every group with p^2 elements for some prime p is abelian. As I stated in Question 2 (vi, and vii). If d is a root of a polynomial $k(x)$ and $f \in Aut(E/Q)$, then $f(d)$ must be a root of $k(x)$. Now $a = \sqrt{3}$, $-a = -\sqrt{3}$ are the roots of $f_a(x) = x^2 - 3$, $b = \sqrt{7}$, -b = - $\sqrt{7}$ are the roots of $f_b(x) = x^2 - 7$. Hence we can now state all elements of $Aut(E/Q)$ (note again that if $h \in Aut(E/Q)$ then h is a field-isomorphism from E ONTO E such that $h(c) = c$ for every $c \in Q$.)

So let $f_1, f_2, f_3, f_4 : E \to E$ be field isomorphisms (note all of them determined by mapping a root of $f_a(x)$ to a root of $f_a(x)$ and a root of $f_b(x)$ to a root of $f_b(x)$. Hence

$f_1(d) = d$ for every $d \in E$ (the identity map), $f_2(a) = -a$ and $f_2(b) = b$ (note that $a = \sqrt{3}$ and $b = \sqrt{7}$), $f_3(a) = a$ and $f_3(b) = -b$, $f_4(a) = -a$ and $f_4(b) = -b$. Now since $|Aut(E/Q)| = 4$. Hence $|f_i)| = 2 or 4$, $i \neq 1$.

Note $|f_1| = 1$ (f_1 is the identity map). It is clear that $[f_i(a)]^2 = f_i(f_i(a)) = a$ and $[f_i(b)]^2 = f_i(f_i(b)) = b$ for every $2 \le i \le 4$. Thus $|f_i| = 2$ for every $2 \le i \le 4$. Hence $Aut(E/Q)$ is isomorphic to $Z_2 \times Z_2$. Thus we have exactly 5 subgroups of $Aut(E/Q)$ (including $\{f_1\}$ and $Aut(E/Q)$. The subgroups are

1) $G_1 = \{f_1\}$ and the corresponding fixed field is E since $f_1(d) = d$ for every $d \in E$ and $|Aut(E/E)| = |G_1| = 1$.

2) $G_2 = \{f_1, f_2\}$ and the corresponding fixed field is $Q(b)$ since $b \notin Q$ and $f_2(b) = b$ and $|Aut(E/Q(b))| = |G_2| = 2 = [E : Q(b)]$.

3) $G_3 = \{f_1, f_3\}$ and the corresponding fixed field is $Q(a)$ since $a \notin Q$ and $f_3(a) = a$ and $|Aut(E/Q(a))| = |G_3| = 2 = [E : Q(a)]$.

4) $G_4 = \{f_1, f_4\}$ and the corresponding fixed field is $Q(ab) = Q(\sqrt{6})$ WHY? since $f_4(a) = -a$ and $f_4(b) = -b$, we have $f_4(ab) = f_4(a)f_4(b) = (-a)(-b) = ab$ and $|Aut(E/Q(ab))| = |G_4| = 2 = [E : Q(ab)]$.

5) $G_5 = Aut(E/Q) = \{f_1, f_2, f_3, f_4\}$ and the corresponding fixed field is Q and $|Aut(E/Q)| = |G_5| = 4 = [E : Q]$.

THUS ALL fields between Q and E are $Q, Q(b), Q(a), Q(ab), E = Q(a, b)$.

QUESTION 7. Let $E = Q(\sqrt{5}, \sqrt{6})$. Find $b \in E$ such that $Q(b) = E$. Find $Irr(b, Q)$.

Solution : By the methods as in Question 4, and 5. We conclude that $[E : Q] = 4$. (Note that $Irr(\sqrt{5}, Q) = x^2 - 5$ and $Irr(\sqrt{6}, Q) = x^2 - 6$).

We claim : $b = \sqrt{5} + \sqrt{6}$

So let

$$x = \sqrt{5} + \sqrt{7}$$

$$x^2 = 12 + 2\sqrt{5}\sqrt{7}$$

$$(x^2 - 12)^2 = (2\sqrt{5}\sqrt{7})^2 = 140$$

$f(x) = Irr(b, Q) = (x^2 - 12)^2 - 140$ **is an Irreducible monic polynomial of degree 4 such that $f(b) = 0$. Hence $[E : Q] = [Q(b) : Q] = 4$ and $Q(b) = E$.**

I end this section with the following amazing result.

QUESTION 8. (nice Question). Prove that if $f(x)$ is a polynomial of degree $n \ge 1$ in $R[x]$ (the polynomial ring with REAL coefficient, then $f(x) = ua_1(x)a_2(x)...a_k(x)$ where u is a nonzero number in R and each $a_i(x)$ is a monic irreducible polynomial of degree 1 or 2 (not necessarily that the $a_i(x)$'s are distinct)

Solution: Since R is a field, we know $R[x]$ is a UFD (Unique factorization domain). Hence we know that $f(x) = ua_1(x)a_2(x)...a_k(x)$ where u is a nonzero number in R and each $a_i(x)$ is a monic irreducible polynomial (not necessarily the $a_i(x)$'s are distinct). The only thing we need to prove that each $a_i(x)$ is of degree 1 or 2. Now $f(x) = x^2 + 1$ is an irreducible polynomial over R and hence $M = (f(x))$ is a maximal ideal of $R[x]$. Thus $R[x]/M$ is a field. Note that $E = R[X]/M = \{a + bx + M | a, b \in R\}$ and $[E : R] = 2$ and $E = span\{1 + M, x + M\}$ over R. Since i is a root of the irreducible polynomial $f(x)$, we know that E is field-isomorphic to $R(i)$ by mapping $x + M$ to i. Hence $R(i)$ is a field and $[R(i) : R] = 2$. Thus $R(i) = span\{1, i\}$ over R. Hence $R(i) = \{a + bi | a, b \in R\} = C$ (the set of all complex numbers). Since $R(i) = C$ and $[R(i) : R] = 2$, we have $[C : R] = 2$. Let $a \in C$. Then the degree of $Irr(a, R)$ must be a factor of $[C : R] = 2$. Hence for every $a \in C$, the degree of $Irr(a, R)$ is either 1 or 2 , i.e, $R[x]$ has no IRREDUCIBLE polynomials of degree ≥ 3. Thus each $a_i(x)$ is a monic irreducible polynomial of degree 1 or 2. Done

2 FINITE FIELDS, fields of characteristic p

Fact 3. (i) Every finite field, say F, has exactly p^n elements for some prime integer p and a positive integer n and $Z_p \subseteq F$. Furthermore, if F_1, F_2 are fields with same number of elements, then F_1, F_2 are isomorphic as FIELD. (Class notes)

(ii) Let F be a finite field with p^n elements. Then $(F^*, .)$ is a cyclic group with $p^n - 1$ elements. Hence $x^{p^n} = x$ for every $x \in F$ (i.e., $x^{p^n} - x = 0$ for every $x \in F$) (class notes)

(iii) Let F be a finite field with p^n elements and $m|n$. Then F has a UNIQUE subfield with p^m elements. Furthermore if H is a subfield of F with p^m elements, then $m|n$ (note that $[F : Z_p] = [F : H][H : Z_p]$) (class notes)

(iv) Let F be a finite field with p^n elements. Let $f(x)$ be an IRREDUCIBLE monic polynomial of degree n in $Z_p[x]$, then F is field-isomorphic to $Z_p[x]/(f(x))$ (class notes).

(v) Let F be a field with p^n elements, $a \in F$. Then a is a root of an IRREDUCIBLE monic polynomial $f(y)$ in $Z_p[y]$ of degree m such that $m|n$. Furthermore, let H be the unique subfield of F with p^m elements, then $f(y)$ splits completely inside H (i.e., $f(y)$ has all its roots (exactly m distinct roots)) and the roots of $f(y)$ are $a, a^p, a^{p^2}, ..., a^{p^{m-1}}$. Also note that $H = Z_p(a) = span\{1, a, a^2, ..., a^{m-1}\}$ over Z_p.

(vi) Let $f(y)$ be an irreducible monic polynomial over Z_p of degree m. Then $f(y)$ splits completely inside a field with p^m elements.

(vii) (in view of the above). Let $f(y)$ be an irreducible monic polynomial over Z_p of degree m. Then the splitting field of Then $f(y)$ splits completely inside a field with p^m elements.

(viii) Let F be a finite field with p^n elements. Then F is a Galois extension of Z_p. Furthermore, $Aut(F/Z_p)$ is a cyclic group with n elements. Hence $|Aut(F/Z_p)| = n$, $Aut(F/Z_p)$ is group-isomorphic to Z_n, and $|Aut(F/Z_p)| = n = [F : Z_p]$. [$Aut(F/Z_p)$ is cyclic, it is trivial, since F has unique subfields of particular order and each subgroup of $Aut(F/Z_p)$ FIXED a unique subfield of F!!)

(ix) THIS RESULT is clear and true for any field F (finite or not). Assume that S_1 be the set of all roots of an IRREDUCIBLE monic polynomial $f(x)$, and S_2 be the set of all roots of an IRREDUCIBLE monic polynomial $h(x)$. If $h(x) \neq f(x)$, then $S_1 \cap S_2 = \emptyset$

(x) (Freshman Dream, class notes). Let F be a finite field with p^n elements. Then for every integer $k \geq 1$ and for every $a, b \in F$, $(a+b)^{p^k} = a^{p^k} + b^{p^k}$

QUESTION 9. Let P_3 be the set of all distinct irreducible monic polynomial of degree 5 over Z_3. Find $|P_3|$ (i.e., HOW MANY MONIC IRREDUCIBLE POLYNOMIALS of degree 5 in $Z_p[y]$ are there?)

Solution: Let $f(y) \in P_3$. By Fact(vi), $f(y)$ has all its roots (exactly 5 distinct roots) inside a field F with 3^5 elements. Let $a \in F$. Then by fact (v) a is a root of a unique monic irreducible polynomial in $Z_3[y]$ of degree m such that $m|5$. Hence Each element in F is a root of an Irreducible polynomial of degree 1 or 5 in $Z_3[y]$. But $Z_3[y]$ has exactly 3 irreducible monic polynomials of degree 1 (namely, y, y + 1, y + 2). Thus each element in $F - Z_3$ is a root of an irreducible monic polynomial of degree 5 in $Z_3[y]$. Now $|F - Z_3| = 3^5 - 3$. By Fact (ix) two distinct polynomials in P_3 have no COMMON root (also note that each polynomial in P_3 has exactly 5 distinct roots in $F - Z_3$). Hence $|P_3| = \frac{3^5-3}{5}$. (nice!)

QUESTION 10. Let P_6 be the set of all distinct irreducible monic polynomial of degree 6 over Z_2. Find $|P_6|$

Solution: Again, let $f(y) \in P_6$. By Fact(vi), $f(y)$ has all its roots (exactly 6 distinct roots) inside a field F with 2^6 elements. Let $a \in F$. Then by fact (v) a is a root of a unique monic irreducible polynomial in $Z_2[y]$ of degree m such that $m|6$. Hence Each element in F is a root of an Irreducible polynomial of degree 1 or 2 or 3 or 6 in $Z_2[y]$. Thus let P_1 be the set of all distinct irreducible monic polynomial of degree 1 over Z_2, let P_2 be the set of all distinct irreducible monic polynomial of degree 2 over Z_2, let P_3 be the set of all distinct irreducible monic polynomial of degree 3 over Z_2, H_2 be the unique subfield of F with 2^2 elements, and H_3 is the unique subfield of F with 2^3 elements. Now by fact (v) each polynomial in P_2 has all its roots (exactly 2 distinct roots) in the subfield H_2 of F and each polynomial in P_3 has all its roots in the subfield H_3 of F. Thus each element in $D = F - (H_3 \cup H_2)$ is a root of an irreducible monic polynomial of degree 6 in $Z_2[y]$ (note that Z_2 is inside every finite finite with 2^n elements, thus if $a \in D$, then $d \notin Z_2$, in fact $H_3 \cap H_2 = Z_2$). Now we calculate $|F - (H_3 \cup H_2|$. First $|H_2 \cup H_3| = |H_2| + |H_3| - |H_2 \cap H_3| = 2^3 + 2^2 - 2 = 10$. Thus $|F - (H_3 \cup H_2)| = 2^6 - 10 = 54$. By Fact (ix) two distinct polynomials in P_6 have no COMMON root (also note that each polynomial in P_6 has exactly 6 distinct roots in $F - (H_2 \cup H_3)$). Hence $|P_6| = 54/6 = 9$ (nice!)

QUESTION 11. Let $f(y) = y^3 + y + 1 \in Z_2[y]$. Show that $f(y)$ is irreducible over Z_2. Find a splitting field of $f(y)$ and write it as a product of linear factors.

Solution: Since $deg(f) = 3$, to show that $f(y)$ is irreducible, it suffices to show that $f(y)$ has no roots in Z_2. Thus since $f(0) \neq 0$ and $f(1) \neq 0$, $f(y)$ is irreducible over Z_2. We know that the splitting field of $f(y)$ is a field with 2^3 elements. Now $M = (f(x)) = (x^3 + x + 1)$ is a maximal ideal of $Z_2[x]$ and $F = Z_2[x]/M$ is a field with 2^3 elements and $F = span\{1 + M, x + M, x^2 + M\}$ over Z_2. Now we "view" $f(y)$ inside $F[y]$ as $f_2(y) = (1+M)y^3 + (1+M)y + (1+M)$ (class notes). We know (class notes) that $x + M$ is a root of $f_2(y)$. Hence by Fact (v), $a_1 = x + M$, $a_2 = x^2 + M$, and $a_3 = x^4 + M$ are all the roots of $f_2(y)$ inside F. Note that if you want then you reduce $x^4 + M$ to $a_0 + a_1x + a_2x^2 + M$ (by dividing x^4 by $x^3 + x + 1$ and taking the remainder). Thus $f_2(y) = ((1+M)y - a_1)((1+M)y - a_2)((1+M)y - a_3)$.

QUESTION 12. Let F be a field with 5^6 elements. Find all elements of $Aut(F/Z_5)$. Find all subgroups of $Aut(F/Z_5)$. For each subgroup H of $Aut(F/Z_5)$ find the corresponding field inside F that is FIXED by H .

Solution: First $|Aut(F/Z_5)| = [F : Z_5] = 6$ and $Aut(F/Z_5)$ is cyclic with 6 elements (isomorphic to Z_6) (see Fact (viii)). We know that $(F, *)$ is a cyclic group with $5^6 - 1$. Thus $(F^*, .) =< a_1 >$ for some $a_1 \in F$ such that $|a_1|_x = 5^6 - 1$. Let $f(y)$ be a monic irreducible polynomial over Z_5 such that $f(a_1) = 0$. Then it is clear that $deg(f) = 6$. Then $f(y)$ has all its roots inside F. Say $a_1 \in F$ is a root of $f(y)$. Then we know that all roots of $f(y)$ are $a_1, a_1^{5^2}, a_1^{5^3}, a_1 5^4, a_1 5^5$ by Fact (v). Let $f \in Aut(F/Z_5)$ (i.e., f is a field-isomorphism from F ONTO F and it fixes Z_p, i.e., f(a) = a for every $a \in Z_p$). Also note that $F = span\{1, a_1, a^2, a^3, a^4, a^5\}$ over Z_5. Then as I discussed in Question 2(vi) f can be determined by mapping a root of $f(y)$ to a root of $f(y)$. Hence let $f_1, f_2, f_3, f_4, f_5, f_6 : F \to F$ be field-isomorphism that fixed Z_p. Then the elements of $Aut(F/Z_5)$ are:

$f_1(b) = b$ for every $b \in F$ (the identity map), $f_2(a_1) = a_1^5$, $f_3(a_1) = a_1^{5^2}$, $f_4(a_1) = a_1^{5^3}$, $f_5(a_1) = a_1^{5^4}$ and $f_6(a_1) = a_1^{5^5}$. We know $Aut(F/Z_5)$ is cyclic. Hence we will find a generator, i.e., at least one of the f_i has order 6 (under composition). Now f_2 (i.e., $f_2(a_1) = a_1^p$) is always such generator. Note that $|a_1| = 5^6 - 1$. and $a_1^{5^6} = a_1$ and 6 is the least positive integer such that $a_1 5^6 = a_1$. Hence clearly that f_2 is a generator of $Aut(F/Z_5)$. For $[f_2(a_1)]^6$ (composition f_2 6 times) = $a_1^{5^6} = a_1$. Thus $Aut(F/Z_5) =< f_2 >$. Since $Aut(F/Z_5)$ is cyclic with 6 elements, $Aut(F/Z_5)$ has exactly one cyclic subgroup of order 1, 2, 3, 6. Since $|f_2| = 6$. Then we know $|[f_2]^2| = |f_3| =$

$6/gcd(2,6) = 3$, $|[f_2]^3| = |f_4| = 6/gcd(3,6) = 2$, $|[f_2]^4| = |f_5| = 6/gcd(4,6) = 3$, $|[f_2]^5| = 6/gcd(5,6) = 6$. **Let** H_2, H_3 **be the unique cyclic subgroups of** $Aut(F/Z_5)$ **of order 2 and 3 respectively. Then** $H_2 = \{f_1, f_4\}$ **and** $H_3 = \{f_1, f_3, f_5\}$. **Thus here are the subgroups:**

1) $H_1 = \{f_1\}$ **and the corresponding fixed field is** E **since** $f_1(d) = d$ **for every** $d \in E$ **and** $|Aut(E/E)| = |G_1| = 1$.

2) $H_2 = \{f_1, f_4\}$. **Let** K_1 **be the field inside** F **that is fixed by each function in** H_2. **We know by Galois Theorem,** $[F : K_1] = |H_2| = 2$. **Since** $[F : Z_5] = [F : K_1][K_1 : Z_5]$ **, we have** $6 = 2[K_1 : Z_5]$ **Thus** $[K_1 : Z_5] = 3$. **Hence** K_1 **is the unique subfield of** F **with** 5^3 **elements.**

3) $H_3 = \{f_1, f_3, f_5\}$. **Let** K_2 **be the field inside** F **that is fixed by each function in** H_3. **We know by Galois Theorem,** $[F : K_2] = |H_3| = 3$. **Since** $[F : Z_5] = [F : K_2][K_2 : Z_5]$ **, we have** $6 = 3[K_2 : Z_5]$ **Thus** $[K_1 : Z_5] = 2$. **Hence** K_2 **is the unique subfield of** F **with** 5^2 **elements.**

4) $H_4 = Aut(F/Z_5) =< f_2 >= \{f_1, f_2, f_3, f_4, f_5, f_6\}$ **and** Z_5 **is the fixed field by each element in** H_4.

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: `abadawi@aus.edu, www.ayman-badawi.com`

2.2 Worked out Solutions for all Assessment Tools

2.2.1 Solution for Exam One

Name——————————————, ID ————————

EXAM I , MTH 532, Spring 2020

Ayman Badawi

QUESTION 1. Given D is a group with 48 elements. Assume that D has an element $a \in C(D)$ such that $|a| = 16$. Prove that D is cyclic.

Solution

By Sylow's Theorems, we must have a subgroup H with 3 elements. Let $h \in H - e$. Then $|h| = 3$. Since $a \in C(D)$, a*h = h*a. Since $a * h = h * a$ and $gcd(|a|, |h|) = gcd(16, 3) = 1$, by a HW problem we conclude that $|b = a * h| = (16)(3) = 48$. Then $D =< b >=< a * h >$. So $D \approx Z_{48}$.

QUESTION 2. Does $U(54)$ have an element of order 18? If yes, how many elements of order 18 does U(54) have?

Solution

$54 = (2)(3^3)$. Hence $\phi(54) = (2)(9)$. By a HW problem $U(54) \approx Z_2 \oplus Z_9 \approx Z_{18}$ (since $gcd(2, 9) = 1$).

By class notes Z_{18} has exactly $\phi(18) = 6$ distinct generators. Since $U(54) \approx Z_{18}$, we conclude that $U(54)$ has exactly 6 elements of order 18.

QUESTION 3. Let $f : (Z_{18}, +) \to (U(50), .)$ be a group homomorphism such that $f(1) \neq 1$. Find $f(0)$. Find $Ker(f)$.

Solution

Note that 0 is the identity of Z_{18} and 1 is the identity of U(50) ($U(50) = \{a \in Z_{50} | gcd(a, 50) = 1\}$ is group under multiplication). Since f is a group homomorphism, we know $f(0) = 1$.

We know $Z_{18}/Ker(f) \approx Range(f) < U(50)$. Now we know by HW problem that $U(50) \approx Z_{20}$.

Thus $Z_{18}/Ker(f) \approx$ to a subgroup of Z_{20}. Thus $m = |z_{18}/kerf| = |Z_{18}|/|Ker(f)|$ must be a factor of 18 and m must be a factor of 20. Hence $m = 1$ or $m = 2$.

If $m = 1$, then $Ker(f) = Z_{18}$ and hence $f(a) = 1$ for every $a \in Z_{18}$, a contradiction since $f(1) \neq 1$. Thus $m =$ 2.

m = 2 implies $2 = |Z_{18}|/|Ker(f)| = 18/|Ker(f)|$. Thus $|Ker(f)| = 9$. Since Z_{18} is cyclic, Z_{18} has unique subgroup with 9 elements. Thus $Ker(f) = \{0, 2, 4, 6, 8, 10, 12, 14, 16\} =< 2 >$.

QUESTION 4. Let D be a group with 100 elements. Assume that D has a subgroup H with 20 elements such that $H \subseteq C(D)$. Prove that D is an abelian group.

Solution

We know $C(D)$ is a normal subgroup of D. Let $m = |C(D)|$. We know that $m|100$. Since C(D) is a group (subgroup of D) and H is a subgroup of D that lives inside $C(D)$, we conclude that H is a subgroup of $C(D)$. Thus 20 | m. Since $20|m$ and $m|100$, we conclude that $m = 20$ or $m = 100$. Assume $m = 20$. Then D/C(D) is a cyclic group (since $|D/C(D)| = 5$). Hence D must be abelian by class notes, and thus $C(D) = D$ and $m = 100$ a contradiction. Hence $m \neq 20$. Thus $m = 100$, and therefore $C(D) = D$. Hence D is abelian.

QUESTION 5. (i) **EXTRA CREDIT, but you need it to solve (ii)**. Let D be a finite group and H be a subgroup of D such that $[D : H] = m$ for some integer m (note that $[D : H] = |D|/|H|$ = number of all distinct left cosets of H). Prove that there is a group homomorphism , say f, from D into S_m such $Ker(f) \subseteq H$.

Solution

Let $L = \{H, a_2 * H, ..., a_m * H\}$ be the set of all distinct left cosets of H.

Now define $f : D \to S_m$ such that $f(a) = \begin{pmatrix} H & a_2 * H & ... & a_m * H \\ a * H & a * a_2 * H & ... & a * a_m * H \end{pmatrix}$ for every $a \in D$.

It is clear that $f(a)$ is a bijective function for every $a \in D$ and thus $f(a) \in S_m$ for every $a \in D$.

It is trivial to check that $f(a * b) = f(a)\ o\ f(b)$ for every $a, b \in D$. Thus f is a group homomorphism.

Let $w \in Ker(f)$. Then $f(w) = \begin{pmatrix} H & a_2 * H & ... & a_m * H \\ w * H & w * a_2 * H & ... & w * a_m * H \end{pmatrix} = \begin{pmatrix} H & a_2 * H & ... & a_m * H \\ H & a_2 * H & ... & a_m * H \end{pmatrix}$. Thus $w * H = H$ and hence $w \in H$. Thus $Ker(f) \subseteq H$. Note that $ker(f) = H$ only if H is a normal subgroup of D. Thus by the first isomorphism theorem , we conclude that $D/Ker(f) \approx$ to a subgroup of S_m.

(ii) Let D be a finite simple group. Assume that H, K are subgroups of D such that $[D : H] = p_1$ and $[D : K] = p_2$ for some prime integers p_1, p_2. Prove that $p_1 = p_2$. (nice result!)

Solution

Let $n = |D|$. First note that p_1, p_2 are prime factors of $|D|$ (i.e., $p_1|n$ and $p_2|n$).

Case 1. Assume $p_2 > p_1$. By part (i), there is a group homomorphism , say f, from D into S_{p_1} such $Ker(f) \subseteq H$. Thus $D/ker(f) \approx$ to a subgroup of S_{p_1}. Since $H \neq D$ and $ker(f) \subseteq H$, we conclude that $Ker(f) \neq D$. Since D is simple and $Ker(f) \neq D$, we conclude that $ker(f) = \{e\}$ and hence $D \approx$ to a subgroup of S_{p_1}.

Note that $|S_{p_1}| = p_1!$. Thus $n|p_1!$. Since $p_2|n$ and $n|p_1!$, we conclude that $p_2|p_1!$, which is impossible since p_2 is PRIME and $p_2 > p_1$ (i.e., p_2 is not a PRIME factor of $p_1!$). Thus $p_2 \ngtr p_1$.

Case 2. Assume $p_1 > p_2$. By similar argument as in case 1. By part (i), there is a group homomorphism , say f, from D into S_{p_2} such $Ker(f) \subseteq K$. Thus $D/ker(f) \approx$ to a subgroup of S_{p_2}. Since $K \neq D$ and $ker(f) \subseteq K$, we conclude that $Ker(f) \neq D$. Since D is simple and $Ker(f) \neq D$, we conclude that $ker(f) = \{e\}$ and hence $D \approx$ to a subgroup of S_{p_2}. Note that $|S_{p_2}| = p_2!$. Thus $n|p_2!$. Since $p_1|n$ and $n|p_2!$, we conclude that $p_1|p_2!$, which is impossible since p_1 is PRIME and $p_1 > p_2$ (i.e., p_1 is not a PRIME factor of $p_2!$). Thus $p_1 \ngtr p_2$.

Since $p_2 \ngtr p_1$ and $p_1 \ngtr p_2$, we conclude that $p_1 = p_2$.

QUESTION 6. Let D be a group with p^m elements, where p is a prime integer and $m \geq 2$. Prove that D has a normal subgroup with p^{m-1} elements. [Hint : Show that D must have a subgroup H with p^{m-1} elements by class note result (which result?). Then use class - lecture (result) to show that H is normal in H (which result?)].

Solution

By Sylow's Theorems (lecture) D has a subgroup with p^i elements for every $1 \leq i \leq m$. Hence D has a subgroup H with p^{m-1} elements. Since $[D : H] = p$ is the smallest prime factor of $|D|$, by class notes we conclude that H is a normal subgroup of D.

QUESTION 7. Let D be a group with $(5^2)(7^2)$ elements. Prove that D is an abelian group. Find all non-isomorphic groups with $(5^2)(7^2)$ elements?

Solution

By Sylow's Theorems, since $n_7 = 1$, we conclude that D has a normal subgroup H with 7^2 elements. Also, since $n_5 = 1$, we conclude that D has a normal subgroup K with 5^2 elements. Since $H \cap K = \{e\}$ and $D = H * K$, by a HW problem we conclude that $D \approx H \oplus K$. Since $|H| = 7^2$, we know (class notes) that H is abelian and thus $H \approx Z_{49}$ or $H \approx Z_7 \oplus Z_7$. Since $|K| = 5^2$, we know (class notes) that K is abelian and thus $K \approx Z_{25}$ or $K \approx Z_5 \oplus Z_5$. Thus D is isomorphic to one and only one of the following groups:

$Z_{49} \oplus Z_{25} \approx Z_{(49)(25)}$ **is cyclic OR**
$Z_{49} \oplus Z_5 \oplus Z_5$ **OR**
$Z_7 \oplus Z_7 \oplus Z_{25}$ **OR**
$Z_7 \oplus Z_7 \oplus Z_5 \oplus Z_5$.

QUESTION 8. Let $a = (1\ 2\ 3)\ o\ (1\ 3\ 4\ 2\ 5) \in S_6$. Is $a \in A_6$? Find $|a|$.

Solution

$a = (2\ 5)\ o\ (3\ 4)$ **is a product of 2 2-cycles. Hence $a \in A_6$. We know $|a| = LCM[2, 2] = 2$.**

QUESTION 9. Let D be a group with 105 elements (105 = (3)(5)(7)).

(i) Prove that D is not simple. [Hint: Assume D is simple. How many elements of orders 7, 5, 3 does D have? is this possible?

Solution

Assume that $n_7 \neq 1$ and $n_5 \neq 1$. Hence we conclude that $n_7 = 15$ and $n_5 = 21$. Thus by a HW problem, D has exactly $(15)(6) = 90$ elements of order 7 and D has exactly $(21)(4) = 84$ elements of order 5. Thus D must have at least 90 + 84 = 174 elements, which is impossible since $|D| = 105$. Hence $n_7 = 1$ or $n_5 = 1$. Thus D has a normal subgroup with 7 elements or a normal subgroup with 5 elements. Thus D is not simple

(ii) Assume that $n_7 = 1$ (i.e., D has exactly one sylow-7-subgroup). Prove that D has a normal cyclic subgroup with 35 elements [hint: Use a result from HW, use a result from class notes! and of course sylow's theorems] .

Solution

Since $n_7 = 1$, we conclude that D has a normal subgroup H with 7 elements. Also, we know that D has a subgroup K with 5 elements. By a HW problem $F = H * K$ is a subgroup of D. Since $H \cap K = \{e\}$, we conclude that $|F| = |H||K| = 35$. Since $[D : F] = 3$ and 3 is the smallest prime factor of $|D|$, by class notes we know that $F = H * K$ is a normal subgroup of D.

Now $|F| = (5)(7)$ and F is a group (subgroup of D), so we can apply sylow's Theorems on F. It is clear that $n_7 = 1$ and $n_5 = 1$. Hence H, K are normal subgroups of F. Since $H \cap K = \{e\}$, by a HW problem we know $F \approx H \oplus K \approx Z_7 \oplus Z_5 \approx Z_{35}$. Hence F is cyclic. Thus F is a cyclic normal subgroup of D.

Submit your solution by 3 pm (as at most), March 28, 2020 .

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: `abadawi@aus.edu, www.ayman-badawi.com`

2.2.2 Solution for Exam Two

Name——————————————, ID ————————

Solution EXAM II , MTH 532, Spring 2020

Ayman Badawi

QUESTION 1. (i) **(3 points)** Let A be a commutative ring with 1 and B be a commutative ring (B may not have "1"). Assume $f : A \to B$ is a ring-homomorphism. Prove that $f(1) \in Id(B)$ (i.e., show that $f(1)$ is an idempotent element of B).

Proof. Since f is a ring-homomorphism, we have $f(1) = f(1._A 1) = f(1)._B f(1) = f(1)^2$. Thus $f(1) \in Id(B)$.

(ii) **(3 points)** Let A be a commutative ring with 1 and $B = 2Z$ (B is the set of all even integers). Assume $f : A \to B$ is a ring-homomorphism. Prove that $f(a) = 0$ for every $a \in A$.

Proof. By part (i), $f(1)$ must be idempotent element of $B = 2Z$. Now $Id(B) = \{0\}$. Thus $f(1) = 0$. Hence $f(a) = f(a._A 1) = f(a)._B f(1) = f(a)._B 0 = 0$ for every $a \in A$.

(iii) **(3 points)** Let A, B be fields and $f : A \to B$ is a ring-homomorphism such that $f(a) \neq 0$ for some $a \in A$. Prove that f is injective (i.e., prove that f is one-to-one).

Proof. By part (i), $f(1_A)$ must be idempotent element of B. Since B is a field, it is clear that $Id(B) = \{0_B, 1_B\}$. Hence $f(1_A) = 0_B$ or $f(1_A) = 1_B$. Assume $f(1_A) = 0$. Then $f(a) = f(a._A 1_A) = f(a)._B f(1) = f(a)._a 0_B = 0$, a contradiction since $f(a) \neq 0_B$. Thus $f(1_A) = 1_B$. We know $Ker(f)$ is an ideal of A. Since A is a field and Ker(f) is an ideal of A, we conclude that $Ker(f) = A$ or $Ker(f) = \{0_A\}$. If $Ker(f) = A$, then $f(b) = 0_B$ for every $b \in A$, which is a contradiction since $f(1_A) = 1_B$. Hence $Ker(f) = \{0_A\}$. Now assume that $f(b) = f(c)$ for some $b, c \in A$. Thus $f(b) +_B -f(c) = 0_B$. Since f is a ring-homomorphism, $f(b +_A -c) = 0_B$. Since $Ker(f) = \{0_A\}$, we conclude that $b +_A -c = 0_A$. Thus $b = c$.

(iv) **(3 points)** Let $f : Z_6 \to Z_9$ be a ring-homomorphism. Prove that $f(a) = 0$ for every $a \in Z_6$.

Proof. Again by part (i), $f(1)$ must be idempotent element of Z_9. By investigation, $Id(Z_9) = \{0, 1\}$. Hence $f(1) = 0$ or $f(1) = 1$. Assume $f(1) = 0$. Then $f(a) = f(a.1) = f(a).f(1) = f(a).0 = 0$ for every $a \in Z_6$ and we are done. Hence assume that $f(1) = 1$. We know that $f(0) = 0$. Hence for every $n \in Z_6$, $0 < n \leq 5$, we have $f(n) = f(1 + ... + 1$ (n times) $) = f(1) + f(1) + ... + f(1)$ (n times) $= n$ (since 9 > 6). Thus $Range(f) = \{0, 1, 2, 3, 4, 5\}$ is a subring of Z_9. In particular, $Range(f)$ is a subgroup of Z_9 UNDER ADDITION. Thus $|Range(f)|$ must be a factor of 9 (Lagrange Theorem for groups), which is impossible since $|Range(f)| = 6$ and 6 is not a factor of 9. Thus $f(1) \neq 1$, and hence $f(1) = 0$. Therefore $f(a) = 0$ for every $a \in Z_6$.

(v) EXTRA (example where $f(1) \neq 0$ and $f(1) \neq 1$) Let $f : Z_6 \to Z_{10}$ be a ring-homomorphism such that $f(a) \neq 0$ for some $a \in Z_6$. Find Range f and $Ker(f)$.

Again by part (i), $f(1)$ must be idempotent element of Z_{10}. By investigation, $Id(Z_{10}) = \{0, 1, 6, 5\}$. Assume that $f(1) = 0$. Hence as before, we conclude that $f(b) = 0$ for every $b \in Z_6$, which is a contradiction since $f(a) \neq 0$ for some $a \in Z_6$. Also as before $f(1) \neq 1$. For if $f(1) = 1$, then $Range(f) = \{0, 1, 2, 3, 4, 5\}$, which impossible since 6 is not a factor of 10. Assume that $f(1) = 6$. Then by calculation, $Range(f) = \{0, 6, 2, 4\}$. Again, it is impossible since $|Range(f)| = 4$ and 4 is not a factor of 10. Now assume that $f(1) = 5$. Then, by calculation , we conclude that f is a ring-homomorphism, $Range(f) = \{0, 5\}$ and $Ker(f) = \{0, 2, 4\}$.

QUESTION 2. (5 points) Let A be a commutative ring with 1 and let I be a proper ideal of A that is not a maximal ideal of A. Hence, we know that $I \subset M$ for some maximal ideal M of A. Let $a \in M - I$. Prove that $a + I$ is not an invertible element of the ring A/I (i.e., show that $a + I \notin U(A/I)$).

Proof First, M is not UNIQUE. Maybe there are infinitely many maximal ideals of A. All of you assumed that M is unique (i.e., M is the only maximal ideal of A) and hence I has to be the maximal ideal M. Note that if you prove that for every nonzero element $a \in A - I$, we have $a + I$ is an invertible element of A/I, then you can conclude that I is a maximal ideal of A.

So, let $a \in M - I$ (note I am not taking $a \in A - I$!) and assume that $a + I$ is invertible in A/I. Thus $a + I.b + I = ab + I = 1 + I$ for some $b \in A$. Hence $1 - ab \in I$. Thus $1 - ab = i \in I$, and hence $1 = ab + i$. Since $a \in M$ and M is an ideal of A and $a \in M$, we conclude that $ab \in M$. Since $I \subset M$, we have $i \in M$. Since $ab \in M$ and $i \in M$, $1 = ab + i \in M$, which is impossible since M is a proper ideal of A ($M \cap U(A) = \emptyset$) (note by definition a maximal ideal is a proper ideal). Thus $a + I$ is not an invertible element of A/I.

QUESTION 3. (5 points) Let A be a finite commutative ring with 1 and $a \in A$. Suppose that $a \notin Z(A)$. Prove that $a \in U(A)$.

Proof. Since A is a finite commutative ring with 1, we may assume that $A = \{0, 1, a_3, ..., a_n\}$. Let $a \in A - Z(A)$. Since A is finite, there exist positive integers $m > k$ such $a^m = a^k$. Thus by distributive law, $a^m = a^k$ implies $a^k(a^{m-k} - 1) = 0$. Since $a \notin Z(A)$, it is clear that $a^f \notin Z(A)$ for every positive integer $f \geq 1$. Thus $a^k(a^{m-k} - 1) = 0$ implies $a^{m-k} - 1 = 0$. Thus $a^{m-k} = 1$. Hence $a \in U(A)$. [THIS is a nice result, so now you have this FACT (add

to your dictionary): If A be a finite commutative ring with 1 and $a \in A$, then EITHER $a \in Z(A)$ OR $a \in U(A)$, A is finite is very CRUCIAL. For let $A = Z$ (A is infinite). Let $a \in A - \{0, 1, -1\}$. Then NEITHER $a \in Z(A)$ NOR $a \in U(A)$]

QUESTION 4. (5 points) Let A be a commutative ring with 1 and $f(X) \in A[X]$ such that $f(X) \neq 0$ and $f(X) \in Z(A[X])$. For every $n \geq 1$, prove that there exists a polynomial $k(X) \in A[X]$ of degree n such that $k(X)f(X) = 0$.

Proof. By Class notes (I-Learn), there exists a nonzero element $b \in Z(A)$ such that $bf(X) = 0$. Let $n \geq 1$ and $k(X) = bX^n$. Then $deg(k(X)) = n$ and by normal multiplications of polynomials, we have $k(X)f(X) = bX^n f(X) = 0$ (since $bf(X) = 0$).

QUESTION 5. (5 points) Let A be a commutative ring with 1 and I be a prime ideal of A. Prove that $Nil(A) \subseteq I$.

Proof. Since I is prime, we know that A/I is an integral domain. Hence $Z(A/I) = \{0 + I\}$. Also note that for any ring B, $Nil(B) \subseteq Z(B)$. Hence let $a \in Nil(A)$. Then $a^n = 0$ for some integer $n \geq 1$. Hence $(a + I)^n = a^n + I = 0 + I$. Thus $a + I \in Nil(A/I)$. Since $Z(A/I) = Nil(A/I) = \{0 + I\}$ and $a + I \in Nil(A/I)$, we conclude that $a + I = 0 + I$. Hence $a \in I$. Thus $Nil(A) \subseteq I$.

another Proof. Let $a \in Nil(A)$. Hence $a^n = 0 \in I$ for some integer $n \geq 2$. Hence $a^n = a.a^{n-1} = 0 \in I$. Thus $a^n = a.a^{n-1} = 0 \in I$. Since I is prime, $a \in I$ or $a^{n-1} \in I$. If $a \in I$, then we are done. Hence assume that $a^{n-1} \in I$ and $n \geq 3$. Since I is prime and $a^{n-1} = a.a^{n-2} \in I$, again we conclude that $a \in I$ or $a^{n-2} \in I$. By repeating as before, we conclude that $a^2 \in I$. Since $a^2 = a.a \in I$ and I is prime, we conclude that $a \in I$.

QUESTION 6. (i) **(3 points)** Let $A = Z_4 \oplus Z_6$. Find all prime ideals of A .

See class notes: $2Z_4 \oplus Z_6$, $Z_4 \oplus 2Z_6$, $Z_4 \oplus 3Z_6$.

(ii) **(3 points). Let $A = Z_{12} \oplus Z_8$. Find $Nil(A)$.**

Note Nil(A) subset of $Z_{12} \oplus Z_8$, i.e., each element in Nil(A) has the form (a, b), where $a \in Nil(Z_{12})$ and $b \in Nil(Z_8)$. By notes, $Nil(Z_{12}) = 6Z_{12} = \{0, 6\}$ and $Nil(Z_8) = 2Z_8 = \{0, 2, 4, 6\}$. Hence $|Nil(A)| = 2.4 = 8$ and $Nil(A) = \{(0, 0), (0, 2), (0, 4), (0, 6), (6, 0), (6, 2), (6, 4), (6, 6)\}$.

(iii) (3 points) Let $B = \begin{bmatrix} 2 & 4 \\ 2 & 2 \end{bmatrix}$. Is B invertible over Z_9? If yes, then find B^{-1}. If No, then explain.

Yes since $|B| = -4 = 5 \in Z_9$ and $5 \in U(Z_9)$ ($gcd(5, 9) = 1$). Since $1/5$ in Z_9 is $5^{-1}.1 = 2.1 = 2$, by class notes $B^{-1} = 2\begin{bmatrix} 2 & -4 \\ -2 & 2 \end{bmatrix} = 2\begin{bmatrix} 2 & 5 \\ 7 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 5 & 4 \end{bmatrix}$.

(iv) (3 points) Let $A = Z_{10}[X]$ and $f(X) = 2X^3 + 5X + 4 \in A$. Is $f(X) \in Z(A)$?

$Z(A) = \{0, 2, 4, 5, 6, 8\}$. **By investigation, $bf(X) \neq 0$ for every nonzero $b \in Z(A)$. Hence, the answer is NO**

(v) (3 points) Give me an example of a commutative ring A with 1 such that $Char(A) = 5$ and $Z(A) \neq \{0\}$.

$A = Z_5 \oplus Z_5$. $Char(A) = LCM(|1|, |1|) = 5$. **Since $(1, 0)(0, 1) = (0, 0)$, we conclude that $Z(A) \neq \{(0, 0)\}$.**

(vi) (3 points) Let $A = Z_{18}[X]$ and $f(X) = 6X^2 + 12X + 17 \in A$. Is there a polynomial $k(X) \in A$ such that $k(X)f(X) = 1$? If yes, then explain (you do not need to find k(X)). If no, then tell me why not.

Since the coefficients of X^2, X in $Nil(Z_{18})$ and $17 \in U(Z_{18})$, by class notes $f(X) \in U(A)$.

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: abadawi@aus.edu, www.ayman-badawi.com

2.2.3 Solution for The Final Exam

Name————————————————, ID ——————————

Final Exam , MTH 532, Spring 2020

Ayman Badawi

QUESTION 1. Let F be a finite field with 2^{12} elements.

(i) **(3 points)** Let $a \in F$. Then a is a root of an irreducible monic polynomial of degree m over Z_2 Find all possibilities of m.

Solution: $m|12$ **implies** $m = 1, 2, 3, 4, 6, 12$

(ii) **(3 points)** We know that $(F^*, .)$ is a cyclic group and hence $(F^*, .) =< a >$ for some $a \in F^*$. Prove that the degree of $Irr(a, Z_2) = 12$? (i.e., prove that the degree of the unique irreducible monic plolynomial over Z_2 that has a as a root is 12)

Solution: Assume degree $Irr(a, Z_2) = m$**. Then we know** $[Z_2(a) : Z_2] = m$**. Thus** $Z_2(a)$ **is a subfield of** F **with** 2^m**. Since** $|a|_x = 2^{12} - 1$**, we conclude that** $m = 12$

(iii) **(3 points)** We know $|F^*| = 2^{12} - 1 = 4095$. Since $819 \mid 4095$, then we know that F^* has a unique cyclic subgroup, say $H =< b >$ for some $b \in F^*$ with 819 elements. What is the degree of $Irr(b, Z_2)$? **justify your answer**

Solution: Assume degree $Irr(b, Z_2) = m$**. Then we know** $[Z_2(a) : Z_2] = m$**. Thus** $Z_2(b)$ **is a subfield of** F **with** 2^m**. Since** $|a|_x = 809$**, we conclude that** $m \neq 1, 2, 3, 4, 6$ **(since** $809 > 2^m$**,** $m = 1, m = 2, m = 3, m = 4, m = 6$**). Thus** $m = 12$

(iv) **(4 points)** Let P_{12} be the set of all irreducible monic polynomials of degree 12 over Z_2. Find $|P_{12}|$. Show the work.

Solution: Since $1 \mid 6, 2|6 , 3|6$**, and** $6|6$**. Every monic irreducible polynomial over** Z_2 **of degree 1 or 2 or 3 or 6 has all its roots in the subfield** H **of** F **with** 2^6 **elements. Hence for every** $a \in W = F - H$**, degree**$(Irr(a, Z_2))$ **is 4 or 12. Thus** $|W = F - H| = 2^{12} - 2^6$**. Hence**

Let K **be the subfield of** F **with** 2^4 **elements and** L **be the subfield of** F **with** 2^2 **elements. Thus each element in** $X = K - L$ **is a root of an irreducible monic polynomial over** Z_2 **of degree 4. Thus** $|X = K - L| = 2^4 - 2^2$**.**

Hence each element in $W - X$ **is a root of an irreducible monic polynomial over** Z_2 **of degree 12.**

Thus $|P_{12}| = |W - X|/12 = (2^{12} - 2^6 - 2^4 + 2^2)/12 = 335$

(v) **(8 points)** Find all elements of the Galois group $Aut(F/Z_2)$. For each subgroup H of $Aut(F/Z_2)$ find the corresponding subfield of F, say L_H, that is fixed by H.

Solution: We know $F^* =< a >$ **and** $a, a^2, a^{2^2}, ..., a^{2^{11}}$ **are the roots of** $Irr(a, Z_2)$ **and** $Aut(F/Z_2) = [F : Z_2] = 12$**. Let** $f_i : F \to F$ **such that** $f_i(a) = a^{2^i}$ **(note** f_0 **is the identity map). Hence** $Aut(F/Z_2) = \{f_0, f_1, ..., f_{11}\}$ **is a cyclic group with 12 elements and it is clear that** $Aut(F/Z_2) =< f_1 >$**. For each** $m|12$ $Aut(F/Z_2)$ **has exactly one subgroup (cyclic) of order** m**.**

For $m = 1, G_1 = \{f_0\}$ **and** F **is the fixed field by** G_1

For $m = 2, G_2 = \{f_0, f_6\}$ **and the unique subfield** H_2 **with** 2^6 **elements is fixed by** G_2 **(note that** $[F : Z_2] = [F : H_2][H_2 : Z_2]$ **and since** $[F : H_2] = 12$ **and** $[F : H_2] = |G_2| = 2$**, we conclude** $[H_2 : Z_2] = 6$**)**

For $m = 3$**,** $G_3 = \{f_0, f_4, f_8\}$ **and the unique subfield** H_3 **with** 2^4 **elements is fixed by** G_3**.**

For $m = 4$**,** $G_4 = \{f_0, f_3, f_6, f_9\}$ **and the unique subfield** H_4 **with** 2^3 **elements is fixed by** G_4

For $m = 6$**,** $G_6 = \{f_0, f_2, f_4, f_6, f_8, f_{10}\}$ **and the subfield** H_6 **with** 2^2 **elements is fixed by** G_6**.**

For $m = 12$**,** $G_{12} = Aut(F/Z_2)$ **and** Z_2 **is the unique subfield fixed by** G_{12}**.**

QUESTION 2. Let E be the 5th cyclotomic extension field of Q

(i) **(2 points)** $E = Q(a)$ for some $a \in C$ (C is the ring (field) of all complex numbers). Find a.

$a = e^{2i\pi/5} = cos(2\pi/5) + sin(2\pi/5)i$

(ii) **(6 points)**Let a as in (i), find $Irr(a, Q)$, find $[E : Q]$, and find all roots of $Irr(a, Q)$ inside E. Is $Aut(E/Q)$ a cyclic group under composition? how many elements does $Aut(E/Q)$ have?

We know $[E : Q] = \phi(5) = 4 = degree(Irr(a, Q))$**. It is clear that** $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$ **and hence** $Irr(a, Q) = f_a(x) = x^4 + x^3 + x^2 + x + 1$**. Also, we know** a, a^2, a^3, a^4 **are the roots of** $f_a(x)$ **(since for every** i**,** $1 \leq i < 5$**, we have** $gcd(i, 5) = 1$ **and thus** $|a^i| = 5$ **for every** $1 \leq i < 5$**). We know** $Aut(E/Q)$ **is group-isomorphic to** $U(5)$ **and since** $U(5)$ **is cyclic, we conclude that** $Aut(E/Q)$ **is a cyclic group with 4 elements.**

(iii) **(2 points)** Find a basis B (in terms of a) of E over Q.

Solution: Since $[Q(a) : Q] = 4$**, we know** $E = Q(a) = span\{1, a, a^2, a^3\}$ **over** Q**.**

(iv) **(2 points)** write $a^6 + a^5 + a^4$ as a linear combination of the elements in the basis B (B is as in iii).

Solution: We know $a^6 + a^5 + a^4$ in $E \leftrightarrow x^6 + x^5 + x^4 + (f_a(x))$ in $Q[x]/(f_a(x))$. Now dividing $x^6 + x^5 + x^4$ by $f_a(x)$ and taking the remainder, we conclude $x^6 + x^5 + x^4 + (f_a(x)) = -x^3 - x^2 + (f_a(x))$ in $Q[x]/(f_a(x))$. Thus $a^6 + a^5 + a^4 = -a^3 - a^2$

(v) **(4 points)** For each subgroup of $Aut(E/Q)$ with 2 elements, say H, find the corresponding subfield of E, say L_H, that is fixed by H.

Solution: Since $Aut(E/Q)$ is a cyclic group with 4 elements $Aut(E/Q)$ has exactly one subgroup with 2 elements, say H. Let I be the identity map on E and $f_4 : E \to E$ such that $f_4(a) = a^4$. Then $H = \{I, f_4\}$ is the unique subgroup of $Aut(E/Q)$ with 2 elements. Since $a + a^4 \notin Q$ and $f_4(a + a^4) = f_4(a) + f_4(a^4) = a^4 + a$, we conclude that $Q(a + a^4)$ is the subfield of E that is fixed by H.

QUESTION 3. Let $E = Q(\sqrt{5}, \sqrt{7})$.

(i) **(3 points)**. We know that $E = Q(a)$ for some $a \in R$. Find $Irr(a, Q)$ (i.e., find the unique irreducible monic polynomial over Q that has a as a root. What is $[E : Q]$?

Solution: We know $a = \sqrt{5} + \sqrt{7}$.

$x = \sqrt{5} + \sqrt{7} \to x^2 = 12 + 2\sqrt{35} \to (x^2 - 12)^2 = 140$. **Hence** $Irr(a, Q) = (x^2 - 12)^2 - 140 = x^4 - 24x^2 + 4$. **Thus $[Q(a) : Q] = 4$.**

(ii) **(3 points)** It is clear that $L = Q(\sqrt{35})$ is a subfield of E. Find the subgroup, say H, of $Aut(E/Q)$ that fixes the field L.

Solution: Since Let I be the identity map on $E = Q(a)$ and $f : E \to E$ such that $f(\sqrt{5}) = -\sqrt{5}$ and $f(\sqrt{7}) = -\sqrt{7}$. It is clear that $H = \{I, f\}$ is the subgroup that fixed the field $L = Q(\sqrt{35})$.

(iii) **(3 points)** Is the field $Q(\sqrt{5})$ isomorphic to the field $Q(\sqrt{7})$? If yes, then construct such ring-isomorphism (field-isomorphism)? If no, then explain briefly why not?

Solution: No. Why? Assume that $f : Q(\sqrt{5}) \to Q(\sqrt{7})$ is a ring-isomorphism. First we know that $f(q) = q$ for every $q \in Q$. Hence f(a root of $x^2 - 5$) must map to a root of $x^2 - 5$. Thus $f(\sqrt{5})$ must be $\sqrt{5}$ or $-\sqrt{5}$. But neither $\sqrt{5}$ nor $-\sqrt{5}$ is in $Q(\sqrt{7})$. Thus such f does not exist.

QUESTION 4. (3 points) Let E be the splitting field of the polynomial $f(x) = x^7 - 18$. We know that E is a Galois Extension of Q. Prove that $Aut(E/Q)$ is a non-abelian group.

Solution: We know that $f(x)$ is irreducible over Q by Einstein's Result. Thus $[E = Q(\sqrt[7]{18}) : Q] = 7$. It is clear that $E \subset R$ and $\sqrt[7]{18}$ is the only real root of $f(x)$. Hence $f(x)$ does not split in E. Since E is not a normal extension of Q, we know by a class result that $Aut(E/Q)$ must be a non-abelian group.

QUESTION 5. (i) **(2 points)** Give me an example of an integral domain that is not a UFD (Unique Factorization Domain).

Let $A = Z + x^2Z[x]$. Then x^2 is an irreducible element of A (note $x \notin A$), but x^2 is not a prime element of A since $x^2 | x^3.x^3$ but $x^2 \nmid x^3$ in A. Thus A can not be a UFD (in a UFD every irreducible element is prime).

(ii) **(2 points)** Give me an example of a Unique Factorization Domain that is not a principal ideal domain.

Solution: We know that $Z[x]$ is a UFD, but the ideal $(x, 2)$ of $Z[x]$ is not a principal ideal

(iii) **(4 points)** Let A be a principal ideal domain. Prove that every prime ideal of A is a maximal ideal of A.[Hint: Every proper ideal is a principal ideal, and every proper ideal is contained in a maximal ideal].

Solution: Let I be a proper ideal of A. We know $I = (a) = aA$ for some prime element a of A. Thus I is contained in a maximal ideal M. Since every maximal ideal is prime, we conclude that $M = (x)$ for some prime element x of A. Since $I \subseteq M$, we conclude that $a = ux$ for some $u \in A$. Since A is a UFD, we know that an element, say b, in A is prime if and only if b is irreducible. Hence a is a irreducible element A. Since a is irreducible and $a = ux$, by definition of irreducible elements, we conclude that $u \in U(A)$ or $x \in U(A)$. Since $M = (x)$, $x \notin U(A)$. Hence $u \in U(A)$. Thus $u^{-1}a = x$. Thus $x \in (a)$, and hence $(x) \subseteq (a)$. Since $(a) \subseteq (x)$ and $(x) \subseteq (a)$, we conclude that $M = (x) = (a) = I$. Thus I is a maximal ideal of A.

(iv) **(4 points)** Let A be a commutative ring with 1. Suppose that A has exactly one maximal ideal. Prove that $Id(A) = \{0, 1\}$. [Hint: note if $x \notin U(A)$, then the ideal $(x) = xA$ is a proper ideal of A].

Solution: Let M be the maximal ideal of A. Assume there is $e \in Id(A)$ such that $e \neq 0, 1$. Hence we know that $1 - e \in Id(A)$. Since (e) and (1 - e) are proper ideals of A and M is the only maximal ideal of A, we conclude that the ideals (e) and $(1 - e)$ "live" inside M. In particular, $e, 1 - e \in M$. Hence $e + 1 - e = 1 \in M$, which is impossible since M is a proper ideal of A. Thus $id(A) = \{0, 1\}$.

(v) **(4 points)** Let A be an integral domain, P be a prime ideal of A, and I be a proper ideal of A such that $I \cap P = \{0\}$. Prove that there exists a prime ideal F of A such that $I \subseteq F$ and $F \cap P = \{0\}$ [Hint: Let $W = P - 0$, note $I \cap W = \emptyset$] **Solution: Let $W = P - \{0\}$. Since A is an integral domain, W is a multiplicative subset of A (i.e., W is a multiplicatively closed subset of A). Since $W \cap I = \emptyset$, we know by a class result, there is a prime ideal F of A that contains I and $F \cap W = \emptyset$. Hence $F \cap P = \{0\}$**

QUESTION 6. (4 points). Let F be a group with 12 elements. Prove that F must have a normal subgroup with 3 elements **OR** F must have a normal subgroup with 4 elements.

Solution : $|F| = 12 = 3.2^2$**. We know to show that** $n_3 = 1$ **or** $n_2 = 1$**. Deny. Then** $n_3 = 4$ **and** $n_2 = 3$**. Now** $n_3 = 4$ **implies that** F **has exactly 8 elements of order 3. Since** $|F| = 12$**, there is a room for one and only one subgroup with 4 elements, a contradiction. Thus** $n_3 = 1$ **or** $n_2 = 1$**. Hence** F **must have a normal subgroup with 3 elements OR** F **must have a normal subgroup with 4 elements.**

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: `abadawi@aus.edu, www.ayman-badawi.com`

2.2.4 Solution for HW-ONE

(HW1, Abstract Algebra)

• Amani Ali Algamez
• 90087115

$\frac{29}{30}$

(i) Let ~~D~~ F be a group and $a \in$ ~~D~~ F. Given $|a| = m < \infty$. Show that $D = \{a, a^2, a^3, \dots, a^m\}$ is a subgroup of ~~D~~ F with m elements.

$|a| = m \to a^m = e$

let $a^k, a^h \in D$ where $h, k \in \mathbb{Z}$, want: $a^{k+h} \in D$

• If $0 \leq k+h \leq m$ then $a^{k+h} \in D$, since $a^0 = a^m = e \in D$

• If $k+h > m$, by division algorithem $\exists\, q \,\&\, r$ s.t

$k+h = qm + r$ where $0 \leq r < m$

now $a^{k+h} = a^{qm+r}$
$= a^{qm} a^r$
$= a^{mq} a^r$
$= e^q a^r$
$= a^r$ since $r < m$ then $a^r \in D$ ✓ (note $a^0 = a^m = e \in D$)

4/4

Hence $a^{k+h} \in D$ and D is closed ∎

(ii) Let D be a group and $a \in D$. Given $|a| = m < \infty$. Assume that $a^n = e$. Prove that $m \mid n$.

$|a| = m \to a^m = e$, want: $m \mid n$

By division algorithem $\exists\, q \,\&\, r$ s.t

$n = qm + r$ where $0 \leq r < m$

given $e = a^n$
$= a^{qm+r}$
$= (a^m)^q a^r$
$= e^q a^r$
$= a^r$

4/4

since m is the smallest integer s.t $a^m = e$ & $r < m$ then $r = 0$

$\to n = qm + 0 \to n = qm \to m \mid n$ ∎

(iii) Let D be a group and $a \in D$. Given $|a| = m < \infty$. Let $b \in D$ such that $b = a^k$ where $\gcd(k,m) = 1$. Prove that $|b| = m$.

$|a| = m \rightarrow a^m = e$

$b = a^k$

$\gcd(k,m) = 1$, want: $|b| = m \rightarrow b^m = (a^k)^m = e$

Let $b^h = e$ for some $h \in \mathbb{Z}$, want to show $h = m$

no no

Assume $|b| = h$, positive integer

This is serious!

$$e = b^h = (a^k)^h = a^{kh} = a^{hk} = (e^h)^k = e$$

now $a^m = e = a^{hk}$

$a^m = a^{hk}$

$m \mid hk$

$m \mid h$ since $\gcd(k,m) = 1$ ✓

$\rightarrow m \leq h$

also, $b^m = (a^k)^m = (a^m)^k = e^k = e \rightarrow h \leq m$

Hence $h = m$ ■

4/5

(iv) Let $D = (\mathbb{Z}_{20}, +)$. Given $H = \{0, 4, 8, 12, 16\}$ is a subgroup of D. Find all left cosets of H.

$a + H = \{a + h \mid h \in H\}$

(1) $0 + H = \{0, 4, 8, 12, 16\} = a_1 + H$

(2) $1 + H = \{1, 5, 9, 13, 17\} = a_2 + H$

(3) $2 + H = \{2, 6, 10, 14, 18\} = a_3 + H$

(4) $3 + H = \{3, 7, 11, 15, 19\} = a_4 + H$

all Left cosets of H.

5/5

(v) Let $D = (\mathbb{Q}, +)$. Then $H = (\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$. Prove that H has infinitely many left cosets. Give me 5 distinct left cosets of H.

let $a \in D$ s.t $0 \leq a < 1$

then there are infinitly many sets $\{a + H\}$

There are left cosets of H of the form:

$a + H = \{ a + h \mid h \in H \ \& \ 0 \leq a < 1 \}$

- Five distinct left cosets:

(1) $0.1 + H$

(2) $0.2 + H$

(3) $0.3 + H$

(4) $0.4 + H$

(5) $0.5 + H$

5/5

(vi) Let $F = \{6, 12, 18, 24\}$ Convince me that F is a group under multiplication module 30 by constructing the Caley's Table. what is e? What is 12^{-1}? what is 24^{-1}?

$\cdot$	6	12	18	24
6	6	12	18	24
12	12	24	6	18
18	18	6	24	12
24	24	18	12	6

5/5

- F is closed under multip. since $\forall a, b \in F$, $a.b \in F$
- $e = 6$, $6.a = a.6 = 6 \quad \forall a \in F$
- $24^{-1} = 24$, $12^{-1} = 18$, $18^{-1} = 12$, $6^{-1} = 6$
- $(a.b).c = a.(b.c) \quad \forall a, b, c \in F$

2.2.5 Solution for HW-Two

Israa Alhamurna MTH 532 HW2 g00081566.

i) Let D be a group, $a \in D$ such that $|a| = n < \infty$. Let m be a positive integer and $r = \gcd(m, n)$. $\Rightarrow |a^m| = n/r$
(proved in solution-book). Just know this fact and use it.

ii) Let $D = (\mathbb{Z}_{24}, +)$. Find $|9|, |14|, |18|, |11|$
(hint: note that $\mathbb{Z}_{24} = \langle 1 \rangle$ and for ex. $8 = 1^8$, then use (i)).

first of all $|D| = |\mathbb{Z}_{24}| = 24$

and since $\mathbb{Z}_{24} = \langle 1 \rangle \Rightarrow |1| = 24$.

- $|9| = |1^9|$ and $|1| = 24$

where $r = \gcd(9, 24) = 3$

1 3 9   1 24 2 12 3 8 4 6.

$r = 3$.

Hence by (i) $\Rightarrow \boxed{|9| = \frac{24}{3} = 8}$

- $|14| = |1^{14}|$ and $|1| = 24$

$r = \gcd(14, 24) \Rightarrow r = 2$.

1 14 2 7.

Hence by (i) $\Rightarrow \boxed{|14| = \frac{24}{2} = 12}$

- $|18| = |1^{18}|$ and $|1| = 24$, $r = \gcd(18, 24)$

1 18 2 9 3 6

$\Rightarrow r = 6$.

by (i) $\Rightarrow \boxed{|18| = \frac{24}{6} = 4}$

- $|11| = |1^{11}|$ and $|1| = 24 \Rightarrow r = \gcd(24, 11)$

$r = 1$

by (i) $\Rightarrow \boxed{|11| = 24}$

iii) Let $a, b \in D$. Assume that $|b| = m < \infty$ prove that $|a^{-1}ba| = m$.

let $|b| = m < \infty$.
and let $|a^{-1}ba| = K < \infty$ for some +ve integer K.

Now, we need to show that $m = K$.

- lets start by:

$|a^{-1}ba| = K$.

$\Rightarrow (a^{-1}ba)^K = \underbrace{(a^{-1}b\cancel{a}) * (\cancel{a^{-1}}b\cancel{a}) * (\cancel{a^{-1}}ba) \cdots * (a^{-1}ba)}_{K \text{ times}} = e.$

identity e

$= (a^{-1}b^Ka) = e$

$\Rightarrow a^{-1}b^Ka = e$. "operate a on both sides"

$b^Ka = a$. "where $a * a^{-1} = e$ and $a * e = a$ $\forall a \in D$ as D is a group."

$\boxed{b^K = e}$ "operate a^{-1} on both sides"

$\boxed{\text{Hence, by H.W(1)} \quad m / K}$ ---- (1)

- Now take,

$(a^{-1}ba)^m = (a^{-1}b\cancel{a}) * (\cancel{a^{-1}}b\cancel{a}) * \cdots * (\cancel{a^{-1}}ba)$ $a * a^{-1} = e$

$= a^{-1}b^ma$

$= a^{-1} * e * a$ "since $b^m = e$".

$= e$

$\boxed{\text{Hence, } K / m \text{ ---- (2)}}$

by (1) and (2) $\Rightarrow$ $m = K$ $\Rightarrow |a^{-1}ba| = m$

(2

Scanned with CamScanner

iv) Let $D = \mathbb{Z}_n \oplus \mathbb{Z}_m$ $n, m \geq 2$

(of course the binary operations are addition mod n and addition mod m).

Let $(a,b) \in D$. Prove that $|(a,b)| = LCM[|a|, |b|]$

[hint: Note that if k, w are integers, then $LCM[k,w] = \frac{kw}{gcd(k,w)}$]

Let $(a,b) \in D$ where $a \in \mathbb{Z}_n$ and $b \in \mathbb{Z}_m$.

and let $|a| = k$ and $|b| = w$

So,

identity of $\mathbb{Z}_n$ under addition.

$\Rightarrow a^k = 0$ mod n.

$\Rightarrow b^w = 0$ mod m

identity of $\mathbb{Z}_m$ under addition.

Now: let $|(a,b)| = t$ --- ①

$\Leftrightarrow (a,b)^t = (a^t, b^t) = (0,0)$.

since by def. k, w are the smallest the integers where $a, b = 0$ respectively. and by H.W ① problem (ii)

$\Rightarrow k / t$ and w / t.

then, t is a common multiple of both k, w --- ②

and If $r = LCM(k,w)$ $\xRightarrow{So,}$ $(a,b)^r = (0,0)$ --- ③

by ① and ③ $\Rightarrow t \leq r$ since t / r.

by ② and ③ $\Rightarrow r \leq t$

$\Rightarrow t \leq r \leq t$

Hence. $t = r$

$|(a,b)| = LCM(k,w)$

$= LCM(|a|, |b|)$ □

(V) Let $D = Z_n \oplus Z_m$

Prove that D is cyclic if and only if $\gcd(n,m) = 1$.

[hint : use part IV].

$\Rightarrow$) let $D = Z_n \oplus Z_m$ is cyclic and prove that $\gcd(n,m) = 1$.

---

since D is cyclic so,

$D = \langle (a,b) \rangle$, $(a,b) \in D$. (a,b) is the generator of D where $Z_n = \langle a \rangle$ and $Z_m = \langle b \rangle$.

then, $|Z_n| = n$, $|Z_m| = m$.

and $|D| = nm$.

- from (iv):

$$|(a,b)| = LCM(|a|, |b|)$$

$$= \frac{|a||b|}{\gcd(|a|, |b|)}$$

$$= \frac{n \cdot m}{\gcd(n,m)} \quad \text{--- } (1)$$

since Z_n, Z_m are cyclic and a, b are there generators respectively, Hence $|a| = n$, $|b| = m$.

- we also know:

$|(a,b)| = nm$ --- (2) since generator of D.

Hence, (1) = (2)

$$\frac{nm}{\gcd(n,m)} = nm$$

$$\Rightarrow \boxed{\gcd(n,m) = 1} \;\blacksquare$$

$\Leftarrow$) Let $\gcd(n,m)=1$, show that D is cyclic:

proof $|\mathbb{Z}_n| = n$, $|\mathbb{Z}_m| = m$, $|D| = nm < \infty$.

let $(a,b) \in D$. and $\mathbb{Z}_n = \langle a \rangle = \{a, a^2, \ldots, a^n = e\}$
$\mathbb{Z}_m = \langle b \rangle = \{b, b^2, \ldots, b^m = e\}$.

Let $|(a,b)| = s < \infty$ for some +ve integer s.

Now by H.W (i)

we can construct a subgroup of D of order s.

s.t

$\{(a,b), (a,b)^2, (a,b)^3, \ldots, (a,b)^s\}$.

- by (iv) $\Rightarrow |(a,b)| = s$

$$= \frac{|a|\,|b|}{\gcd(|a|,|b|)}$$

$$= \frac{nm}{\gcd(n,m)}$$

$$= \frac{nm}{1} \text{ given.}$$

$\Rightarrow |(a,b)| = s = nm = |D|$

$\{(a,b), (a,b)^2, \ldots, (a,b)^{nm}\}$

Hence, $D = \langle (a,b) \rangle$.

$\Rightarrow$ D is cyclic. ■

vi) Let $D = \mathbb{Z}_6 \oplus \mathbb{Z}_{14}$

a) convince me that D is not cyclic. Find the value of integer m such that the order of each element in D is $\leq m$

$\gcd(6,14) = 2 \neq 1$, Hence, by (V) D is Not cyclic.

as D is of the form $\mathbb{Z}_n \oplus \mathbb{Z}_m$ and it is an ~~iff~~ statement. [also, note part (d) gives a counter example if we assume D is cyclic]

$|D| = |6(14)| = 84$. and by Thm in class

if $(a,b) \in D$ then $|(a,b)| \,/\, |D|$

$|(a,b)| \,/\, 84 \Rightarrow \left[1, \cancel{84}, 2, 42, 3, 28, 4, 21, 6, 14, 7, 12 \right]$ possible orders of (a,b)

Not cyclic.

also, by iv)

$|(a,b)| = LCM(6,14) = \frac{84}{2} = 42$

$\Rightarrow \boxed{m = 42.}$

the least common multiple of both the max order of an element a in $\mathbb{Z}_6 = 6$. and the max order of an element b in $\mathbb{Z}_{14} = 14$.

(b) Find $|(3,5)|$ and $|(4,10)|$

[Hint : note $3 = 1^3$ and $5 = 1^5$. Now use (i) and (iv)].

- $|(3,5)| = \dfrac{|3| \cdot |5|}{gcd(|3|, |5|)}$ --- by (iv).

$|3| = |1^3|$ since $Z_6 = \langle 1 \rangle$ as $3 \in Z_6$.

and $|1| = 6$.

$\Rightarrow gcd(3,6) = 3$

Hence by (i) $\Rightarrow |3| = \frac{6}{3} = \boxed{2}$

Now,

$|5| = |1^5|$ since $Z_{14} = \langle 1 \rangle$ and $5 \in Z_{14}$

$|1| = 14$, $gcd(5,14) = 1$

$|5| = \boxed{14}$

$\Rightarrow \boxed{|(3,5)| = \dfrac{2 \cdot 14}{gcd(2,14)} = \dfrac{\cancel{2} \cdot 14}{\cancel{2}} = \boxed{14}}$

- $|(4,10)|$:

$|4| = |1^4|$ and $|1| = 6$.

$gcd(4,6) = 2$

$\Rightarrow |4| = \frac{6}{2} = \boxed{3}$.

$|10| = |1^{10}|$ and $|1| = 10$.

$gcd(10,14) = 2$.

$|10| = \frac{14}{2} = \boxed{7}$

$\Rightarrow \boxed{|(4,10)| = \dfrac{|4| \, |10|}{gcd(|4|, |10|)} = \dfrac{3 \cdot 7}{1} = \boxed{21}}$

Scanned with CamScanner

(c) Give me two subgroups of D. say H_1, H_2 such that $|H_1| = |H_2| = 2$.

$Z_6 = \{0,1,2,3,4,5\} \oplus Z_{14} = \{0,1,2,\cdots,13\}$.

$(a,b) \in H_1$ or H_2.

$|(a,b)| \,/\, |H_1|$ or $|H_2|$

$|(a,b)| \,/\, 2 \Rightarrow |(a,b)| = 2. \rightarrow LCM(|a|,|b|)$

where $a \in Z_6$ and $b \in Z_{14}$.

Hence $|a| = 2 \mod 6$.

$\Rightarrow a = 3$

$|b| = 2 \mod 14 \Rightarrow b = 7$.

to check $|element| = 2$.

$$\boxed{\begin{aligned} H_1 &= \{(0,0), (3,7)\} \\ H_2 &= \{(0,0), (3,0)\} \end{aligned}}$$

$\rightarrow (3,7)^2 = (3^2, 7^2) = (0,0)$ ✓

$\rightarrow (3,0)^2 = (0,0)$ ✓

(d) does D have a cyclic subgroup of order 21?
If yes find a generator to such group.

① D is an abelian group and 21/84
$\Rightarrow$ so D has a subgroup of order 21

② from part (b) $|(4,10)| = 21$, then by H.W①
we can have a subgroup as $\{(4,10), (4,10)^2, \cdots, (4,10)^{21}\}$
$\Rightarrow$ The subgroup is cyclic
and $(4,10)$ can be a generator of such a subgroup.
$|(4,10)| = |subgroup|$.

or in general:

$(a,b)^{21} = (0,0)$

$(a^{21}, b^{21}) = (0,0)$. $a \in \mathbb{Z}_6$ and $b \in \mathbb{Z}_{14}$.

$|a| / 21$ and $|b| / 21$. and $\gcd(|a|, |b|) = 1$ to be cyclic (V)

and since $1 \leq |a| \leq 6$, $1 \leq |b| \leq 14$.

$|a| = \underline{\underline{3}}$, $|b| = 3, \underline{\underline{7}}$.

Hence, $(2,2)$. is another example of the generator of a cyclic subgroup of order 21.

$\Rightarrow$ [Yes, D has a cyclic subgroup of order 21 and examples of the generator. (2,2) and (4,10).]

★ Note. for part (a):-

this can be another way to prove that D is Not cyclic, where if we assume D cyclic the contradiction appears since we have 2 different subgroups of the same size (Not unique) Hence, D is Not cyclic.

Scanned with CamScanner

2.2.6 Solution for HW-Three

Israa Alhamarna   MTH 532   g00081566.

H.W 3

(i) Fact: (for a proof just see it in any Algebra Text Book).
Let H be a subset of a group D. (note that H can be infinite or finite). Then H is a subgroup of D iff $a^{-1} * b \in H$ for every $a, b \in H$. (a, b need Not to be distinct).

(ii) Let F, L be subgroups of a group D. Prove that $M = F \cap L$ is a subgroup of D. (hint: use (i) above).

we know $F, L \leq D$ (F, L subgroups of D)
Want to show that if a, b any 2 elements in M, then $a^{-1} * b \in M$.

Proof: let $a, b \in M$ since $M = F \cap L$, then

$a, b \in F$ and $a, b \in L$.

$a^{-1} \in F$ and $a^{-1} \in L$ " since by the def. of the group or (subgroup) for each $a \in F, L$ $\exists a^{-1}$ unique s.t $a^{-1} \in F, L$."

now, $\forall a, b \in F, L$.

$a^{-1} * b \in F$ and

$a^{-1} * b \in L$ since subgroups of D by (i)

Hence
$\Rightarrow a^{-1} * b \in M$. " intersection of F and L"

So, M is a subgroup of D. ∎

5/5

(1)

(iii) by (ii), $N = 12\mathbb{Z} \cap 15\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$.

Since $\mathbb{Z}$ is cyclic, we know $N = a\mathbb{Z}$, find a.

using a class-Note.

Every subgroup of $(\mathbb{Z}, +) = \langle \hat{1} \rangle$ for some $n \in \mathbb{Z}$.

$12\mathbb{Z} = \langle 12 \rangle = \langle 1^{12} \rangle$

$15\mathbb{Z} = \langle 15 \rangle = \langle 1^{15} \rangle$ 5/5

15: 3, 5   12: 3, 2, 2

$N = 12\mathbb{Z} \cap 15\mathbb{Z}$

$= LCM(12, 15)\mathbb{Z}$

$= 60\mathbb{Z} = \langle 1^{60} \rangle$.

$LCM = 3 \cdot 5 \cdot 2 \cdot 2 = 60$.

$\Rightarrow \boxed{a = 60}$

iv) Let D be an abelian group with 9 elements. Given that D has two distinct subgroups, H_1, H_2 such that $|H_1| = |H_2| = 3$. Convince me that it is impossible that $D = (\mathbb{Z}_9, +)$. What will be an example of such group D?

$(\mathbb{Z}_9, +)$ is cyclic group, so although it is abelian of 9 elements it is impossible that it has more than one unique subgroups of the same order $(3 \mid 9)$ and since D here has 2 distinct subgroups of order 3 then D can't be $(\mathbb{Z}_9, +)$. 5/5

$gcd(3,3) \neq 1$

$\boxed{D = \mathbb{Z}_3 \oplus \mathbb{Z}_3}$ (by H.w 2) is an example of such D, where it is abelian, Not cyclic

- $|D| = 9$

example of subgroups.

$H_1 = \{(0,0), (1,2), (2,1)\}$

$H_2 = \{(0,0), (1,1), (2,2)\}$

$|H_1| = |H_2| = 3$, where $H_1 \neq H_2$.

(2)

· (V) Let $f \in S_n$ such that f is m-cycle. Convince me that if m is odd integer, then $f \in A_n$, and if m is an even integer then $f \notin A_n$

Let $f = \overset{\to\, m\text{-cycle}}{(a_1 \; a_2 \; \cdots \; a_m)} \in S_n$.

• We know by Class-Theorem that any bijective function $f \in S_n$ can be written as Composition of 2-cycles as following:

$$f = (a_1 \; a_2 \; \cdots \; a_m) = \underbrace{(a_1 \; a_m)(a_1 \; a_{m-1}) \cdots (a_1 \; a_2)}_{(m-1)\ 2\text{-cycles}}$$

• by staring and few exampls like:

$$(a_1 \; a_2 \; a_3) = \underbrace{(a_1 \; a_3)(a_1 \; a_2)}_{2\ 2\text{-cycles}}$$

$$(a_1 \; a_2 \; a_3 \; a_4 \; a_5 \; a_6) = \underbrace{(a_1 \; a_6)(a_1 \; a_5)(a_1 \; a_4)(a_1 \; a_3)(a_1 \; a_2)}_{5-2\text{cycles}}$$

(*) We notice that f can be written as $\boxed{(m-1)\ 2\text{-cycles}}$

Hence,

• when m is odd $\Rightarrow$ $(m-1)$ is even $\Rightarrow$ $f \in A_n$.

• when m is even $\Rightarrow$ $(m-1)$ is odd $\Rightarrow$ $f \notin A_n$.

5/5

(3)

vi) let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 6 & 8 & 7 & 2 & 1 & 5 \end{pmatrix} \in S_8$.

(a) Find $|f|$. Is $f \in A_8$? Explain.

$$f = \overbrace{(1\ 4\ 8\ 5\ 7)}^{c_1}\overbrace{(2\ 3\ 6)}^{c_2}$$

2 disjoint cycles, so by class Thm.

$$|f| = \text{LCM}(\text{legth of } c_1, \text{length of } c_2)$$
$$= \text{LCM}(5, 3)$$
$$= \boxed{15}$$

3/3

- $f = (1\,4\,8\,5\,7)(2\,3\,6)$

odd - cycle → even 2-cycle.   odd - cycle → even 2-cycle

→ even · even = even ⇒ $f \in A_8$ as $f \in S_8$ by (V).

Also,

$$f = (14857)(236)$$
$$= \underbrace{(1\,7)(1\,5)(1\,8)(1\,4)(2\,6)(2\,3)}_{6-2 \text{ cycles}}$$

Since f can be written as even number of 2-cycle

So, Yes $f \in A_8$ since by Class Thm if f cycle can be written as an even number of 2-cycles then it $\in A_n$ (the subgroup of S_n) and can't be off odd 2-cycles.

continue VI)

*(b) Does A_8 has an abelian subgroup with 15 elements.
[Hint : If you show that A_8 has a cyclic subgroup with 15 elements, then you are done, since cyclic implies abelian].

In order to show abelian subgroup.
we need to find a cyclic subgroup with 15 elements.
and to do so,
we should show that $\exists$ element $f \in A_8$ s.t

$|f| = 15$

$= LCM(\text{length of } C_1, \text{length of } C_2)$ — C_1, C_2 disjoint cycles.

$= LCM(5, 3)$

$= (1\,2\,3\,4\,5)(6\,7\,8)$

$= 15$.

15: 1, 15, 3, 5

Hence, by H.W (F)
$\exists$ a cyclic subgroup $\langle f \rangle$ s.t:
$\{f, f^2, f^3, ----, f^{15}\}$

$\Rightarrow$ A_8 has a cyclic subgroup of 15 elements so, it has an abelian subgroup of 15 elements since cyclic emplies abelian.

5/5

vii) let $f=\underbrace{(143)(14)}_{\text{not disjoint}} \in S_4$. Find $|f|$. let $k=\underbrace{(143)(15)}_{\text{not disjoint}} \in S_5$ find $|k|$.

$$f=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \Rightarrow f=(1\ 3)$$

$\boxed{|f|=2}$

$$k=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix} \Rightarrow k=(1\,5\,4\,3)$$

$\boxed{|k|=4}$

viii) Given $H=\{(1),(143),(134)\}$ is a subgroup of S_5. (this is given, you do not need to check). Find the left coset $(15)\circ H$ and find the right coset $H\circ(15)$. What do you observe? Can we say that H is a normal subgroup of S_5?

* left coset: $(15)\circ H=\{(15)(1),(15)(143),(15)(134)\}$

- $(15)(143)=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}=(1435)$
- $(15)(134)=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix}=(1345)$

$\Rightarrow (15)\circ H=\{(15),(1435),(1345)\}$

* right coset: $H\circ(15)=\{(1)(15);(143)(15),(134)(15)\}$

- $(143)(15)=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix}=(1543)$
- $(134)(15)=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix}=(1534)$

$\Rightarrow Ho(15) = \{(15), (1543), (1534)\}$. 5/5

we notice that $(15) \circ H \neq H \circ (15)$

Hence H can't be a normal subgroup of S_5

Since $\exists\ (15) \in S_5$ where left coset $\neq$ right coset

which gives a counter example and according to class-Note

it is enough to show not normal subgroup.

(ix) Let a, b be element of a group such that $a*b = b*a$

Assume $|a| = n$ and $|b| = m$. let $k = |a*b|$. Prove k/nm.

$a*b = b*a$ for $a, b \in D$. $\Rightarrow a*b \in D$ (by group closure under $(*)$ operation)

let $|a| = n$ and $|b| = m$.

and $|a*b| = k$. $\Longleftrightarrow a^n = e$, $b^m = e$ and $(a*b)^k = e$.

Now,

$$\Rightarrow (a*b)^{nm} = \underbrace{(a*b)(a*b)(a*b) \cdots (a*b)}_{nm \text{ times}} \quad \text{given}$$

$$= (a*a)(b*a)(b*b) \cdots (b*b) \quad \Rightarrow \text{since } a*b = b*a$$

$$= \underbrace{(a*a* \cdots *a)}_{nm \text{ times}} \underbrace{(b*b* \cdots b)}_{nm \text{ times}}$$

$$= a^{nm} * b^{nm}$$

$$= (a^n)^m * (b^m)^n$$

"or by H.W(1) since n/nm and m/nm"

$$= (e)^m * (e)^n$$

$$= e$$

5/5

$$\Rightarrow (a*b)^{nm} = e$$

Hence, by H.W(1) k/nm. □

(X) Give me an example of two elements a, b in a group where $|a| = n$, $|b| = m$ and $|a*b| = k$ but $k \nmid nm$.
[hint: Stare at the element K in vii and somehow find a, b].

let the group be S_5

$K = (143)(15) \in S_5$.

$a = (143) \in S_5$ and $b = (15) \in S_5$.

$|a| = 3 = n$, $|b| = 2 = m$

$K = a * b = (143)(15)$ $\quad (* = \circ)$

$|K| = 4$.

$nm = 3 \cdot 2 = 6$

$\Rightarrow \boxed{4 \nmid 6.}$

xi) let a, b be element of a group such that $a*b = b*a$
Assume $|a| = n$, $|b| = m$ and $\gcd(n, m) = 1$. let $k = |a*b|$
Prove $k = nm$ [Hint: you may want to use the fact from number Theory that if $\gcd(w, d) = 1$, $d \mid c$ and $w \mid c$ then $wd \mid c$ where w, d, c are the integers].

- by (ix) we know that if $a, b \in D$ where $a*b = b*a$ $|a| = n$ and $|b| = m$ and $|a*b| = k$ then $\boxed{K / nm}$ --- 1
- So we only need to show nm / K.

since $a*b = b*a$

$|a*b| = k \Leftrightarrow (a*b)^k = e \Rightarrow a^k * b^k = e$

$\Rightarrow a^{kn} * b^{kn} = e$ for the integer n

$\Rightarrow (a^n)^k * b^{kn} = e \Rightarrow e * b^{kn} = e \Rightarrow b^{kn} = e$

Hence, m / kn but $\gcd(m, n) = 1$

$\Rightarrow \boxed{m / k}$ ✓ Good!

8

Now, Similarly for m +ve integer. $(a^k * b^k)^m = a^{km} * b^{km} = e^m = e$
since $ab = ba$.

$a^{km} * b^{km} = e$

$a^{km} * (b^m)^k = e \Rightarrow a^{km} * e^k = e$

$\Rightarrow a^{km} = e$.

5/5

Then, n / km and $\gcd(n,m) = 1$

$\Rightarrow \boxed{n / k}$

using the hint, m/k, n/k, and $\gcd(n,m)=1$.

$\Rightarrow \boxed{mn / k}$ -- ②

by ① and ② $\boxed{k = nm}$ ∎

xii) Let $F : (D_1, *_1) \longrightarrow (D_2, *_2)$ be a group-homomorphism and $H < D_1$. Prove that $F(H)$ is a subgroup of D_2. (note it is possible that $H = D_1$) [Hint: use part (i) above].

<u>Want</u> to show that $[F(a)]^{-1} * F(b) \in F(H)$

$\forall F(a), F(b) \in F(H)$, $a, b \in H$

Now, we know $H < D_1$, then by (i) we know H is not empty $\Rightarrow F(H) \neq \emptyset$.

$a^{-1} *_1 b \in H \quad \forall a, b \in H$

and $F(a *_1 b) = F(a) *_2 F(b) \quad \forall a, b \in D_1$

and as $H < D_1$, then, $\forall a, b \in H$

$[F(a *_1 b) = F(a) *_2 F(b)] \in F(H)$

since $\forall a \in H, \exists\, a^{-1}$ unique $\in H$.

Hence,

$F(a^{-1} *_1 b) = F(a^{-1}) *_2 F(b)$ "by class-big Thm"

$= [F(a)]^{-1} *_2 F(b) \Big\} \in F(H)$

$\Rightarrow F(H)$ is a subgroup of D_2 ∎

xiii) Let $F : (\mathbb{Z}_{24}, +) \longrightarrow (\mathbb{Z}_{15}, +)$ be a group homomorphism such that $F(1) \neq 0$. Find $F(\mathbb{Z}_{24})$. [Hint: Note that $\mathbb{Z}_n$ is cyclic, $F(\mathbb{Z}_{24})$ is a subgroup of $\mathbb{Z}_{15}$ by xii and $|F(a)|$ must be a factor of $|a|$ for every $a \in \mathbb{Z}_{24}$ by Class-Theorem].
Find $F(1)$, $F(8)$, $F(12)$.

$F : (\mathbb{Z}_{24}, +) \longrightarrow (\mathbb{Z}_{15}, +)$

$F(a + b \bmod 24) = (F(a) + F(b)) \bmod 15$

$\mathbb{Z}_{24} = \{0, 1, 2, 3, \dots, 23\}$, $\mathbb{Z}_{15} = \{0, 1, 2, \dots, 14\}$.

$F(\mathbb{Z}_{24}) < \mathbb{Z}_{15}$ (by xii)

- by lagrange $|F(\mathbb{Z}_{24})| \,/\, 15$ order of $\mathbb{Z}_{15}$ (cyclic)
- Also, by class big Thm $|F(a)| \,/\, |a|$ $\forall a \in \mathbb{Z}_{24}$ and since $\mathbb{Z}_{24}$ is cyclic $\Rightarrow |F(\mathbb{Z}_{24})| \,/\, 24$

(*) factors of 15: 1, 15, 3, 5
factors of 24: 1, 24, 2, 12, 3, 8, 4, 6.

Hence, by (*) $|F(\mathbb{Z}_{24})| = 1$ or 3.

Now, by class - Most important Result after Lagrange.
we have

(**) -- $f : (\mathbb{Z}_{24}/\ker(F), \Delta) \longrightarrow F(\mathbb{Z}_{24})$

where $\mathbb{Z}_{24}/\ker(F) \simeq F(\mathbb{Z}_{24})$.

Hence, $|F(\mathbb{Z}_{24})| \neq$ since if $|F(\mathbb{Z}_{24})| = 1$, then

$|\mathbb{Z}_{24}/\ker(F)| = 1 \Rightarrow \mathbb{Z}_{24} = \ker(F)$

which means $\forall a \in \mathbb{Z}_{24} \Rightarrow F(a) = 0$ contradiction since given $F(1) \neq 0$.

Hence, we are only left with

$|F(\mathbb{Z}_{24})| = 3$. and , $\frac{15}{3} = 5$.

then $\boxed{F(\mathbb{Z}_{24}) = \{0,5,10\} < \mathbb{Z}_{15}}$

subgroup of cyclic so, cyclic.

$\boxed{F(\mathbb{Z}_{24}) = \{0,5,10\} = 5\mathbb{Z}_{15}}$.

Answer.

since $\mathbb{Z}_{15}$ is cyclic then $\{0,5,10\}$ is a unique subgroup of order 3, Hence

- $\boxed{F(1) = 5}$ mod 15
- $\boxed{F(8) = F(1^8) = [F(1)]^8 = 40 \bmod 15 = 10}$
- $\boxed{F(12) = F(1^{12}) = [F(1)]^{12} = 60 \bmod 15 = 0}$

OR to show this in details using (**)

$\frac{24}{8} = 3$ $\quad \left| \mathbb{Z}_{24}/Ker(F) \right| = 3 \Rightarrow |Ker(F)| = 8$

and since $Ker(F) = \{ b \in \mathbb{Z}_{24},\ F(b) = 0 \bmod 15 \}$

$Ker(F) = \{0,3,6,9,12,15,18,21\}$

$\mathbb{Z}_{24}/Ker(F) = \{ \underbrace{Ker(F)}_{0}, \underbrace{1+Ker(F)}_{5}, \underbrace{2+Ker(F)}_{10} \}$

- $f(1+Ker(F)) = F(1)$

$1+Ker(F) = \{1,4,7,10,13,16,19,22\}$

we notice that any element in $1+Ker(F) \longrightarrow 5$ in $F(\mathbb{Z}_{24})$.

$\Rightarrow \boxed{F(1) = 5}$

Properties of Cosets

- $F(12) = f(12+Ker(F)) = f(Ker(F))$ since $12 \in Ker(F)$

$\Rightarrow \boxed{F(12) = 0}$

- $F(8) = f(8+Ker(F)) = f(2+Ker(F))$

as $2+Ker(F) = \{2,5,8,11,14,17,20,23\}$ so, $8 \in 2+Ker(F)$.

$\Rightarrow \boxed{F(8) = 10}$ $\quad 2+Ker(F) \longrightarrow 10$ in $5\mathbb{Z}_{15}$ or $F(\mathbb{Z}_{24})$

5/5 ✓

2.2.7 Solution for HW-Four

Israa Alhamerna

MTH 532
H.W4

g00081566,

Q1) (i) Let D be a group with 27 elements. You just observed that $C(D)$ has at least 4 elements. Prove that D is abelian.

$|D| = 27$, given $|C(D)| \geq 4$.

want to prove that $\frac{D}{C(D)}$ is cyclic. Hence, by class result

D is abelian.

Now,

$\Rightarrow$ From class notes, we know.

$C(D) < D$, Hence by Lagrange. as $D < \infty$.

$|C(D)| \mid |D|$ then,

$|C(D)| = 1, 3, 9, 27$ but can't be $|C(D)| \neq 1$ or 3.

since given $|C(D)| \geq 4$.

So we are only left with $|C(D)| = 9, 27$.

① if $|C(D)| = 27$

$\Rightarrow C(D) = D$ then by the Definition of $C(D)$.

D is abelian since all elements of D are center elements.

② if $|C(D)| = 9$.

$\Rightarrow \left|\frac{D}{C(D)}\right| = \frac{|D|}{|C(D)|} = \frac{27}{9} = \boxed{3} \rightarrow$ prime, so

$\frac{D}{C(D)}$ is cyclic by class notes and then, by

Class Theorem D is abelian.

by ① and ② $\Rightarrow \blacksquare$.

(iii) Let D be a finite group, K, H are normal subgroups of D such that $H * K = D$ and $H \cap K = \{e\}$.

(a) prove that $K \approx D/H$

[Hint note that $|D/H| = |K|$. define $f : K \to D/H$ such that $f(k) = k * H$ for every $k \in K$. Show that f is group homorphism and then you only need to show that f is 1-1]

Let $f : K \to (D/H, \Delta)$ such that $\boxed{f(k) = k * H}$ for every $k \in K$

$K \lhd D$.

- to show homorphism:

let $k_1, k_2 \in K$, want $f(k_1 * k_2) = f(k_1) \Delta f(k_2)$

$f(k_1 * k_2) = (k_1 * k_2) * H$ "by Def of $(\frac{D}{H}, \Delta)$"

$= k_1 * H \Delta k_2 * H$

$= f(k_1) \Delta f(k_2)$ □

$\boxed{\text{Hence } f \text{ is homorphism}}$ -- ①

- since $|D/H| = |K|$ then 1-1 is enough for f to be bijective:

so, let $f(k_1) = f(k_2)$ for any $k_1, k_2 \in K$

$(k_1 * H = k_2 * H) \times k_2^{-1}$

Now, $k_2^{-1} * k_1 * H = H$

so, $k_2^{-1} * k_1 \in H$ "by Def of cosets"

we also know that, by K being a subgroup.

$k_2^{-1} * k_1 \in K$ $\forall k_1, k_2 \in K$ → since $k_2^{-1} \in K$.

Now, since given $H \cap K = \{e\}$ ⇒ the only common element of K and H is e

but we showed that $k_2^{-1} * K \in H$ and K.

$\Rightarrow k_2^{-1} * k_1 = \{e\} \to k_1^{-1} = k_2^{-1}$ "uniqueness of inverse" in group.

$\boxed{k_1 = k_2}$

Thus, f is 1-1 --- 2

by 1 and 2 $\quad K \approx D/H$.

(b) prove $H \approx D/K$.

Let $g : H \longrightarrow (D/K, \Delta)$ s.t $(g(h) = h * K)$ $\forall h \in H$. (*)

- $\boxed{\text{Homorphism}}$: by (*)

$$g(h_1 * h_2) = (h_1 * h_2) * K \quad \text{for any } h_1, h_2 \in H.$$

$$= (h_1 * K) \Delta (h_2 * K) \quad \text{"Def of } D/K\text{"}$$

$$= g(h_1) \Delta g(h_2) \quad \square \text{ 1}$$

- $\boxed{1-1}$ $\quad |K| = |D/K|$

it is enough to show g is 1-1, to be bijective.

so, for any $h_1, h_2 \in H \trianglelefteq D$

Let $g(h_1) = g(h_2)$

$(h_1 * K = h_2 * K) \quad * h_2^{-1}$

$\underbrace{h_2^{-1} * h_1}_{\in H} * K = K \quad \Rightarrow h_2^{-1} * h_1 \in K \quad$ "Def of cosets $\frac{D}{K}$".

we also know, since $H < D$, $\forall h_1, h_2 \in H$

$h_2^{-1} * h_1 \in H \quad$ since $h_2^{-1} \in H$.

But given $H \cap K = \{e\}$

$\Rightarrow h_2^{-1} * h_1 = \{e\}$

$h_1^{-1} = h_2^{-1}$ by uniquness of inverse.

$\boxed{h_1 = h_2}$ --- 2

by 1 and 2 $\quad H \approx D/K$.

$$(G, \Delta_3)$$

(c) Prove that $D \approx \underbrace{\frac{D}{H}}_{(\frac{D}{H}, \Delta_1)} \oplus \underbrace{\frac{D}{K}}_{(\frac{D}{K}, \Delta_2)} \approx K \oplus H.$

Let $f : D \longrightarrow \frac{D}{H} \oplus \frac{D}{K}$ where for $\forall d \in D$.

$f(d) = (d * H, d * K)$.

- <u>Homorphism</u> :-

for any $d_1, d_2 \in D$.

$f(d_1 * d_2) = \Big((d_1 * d_2) * H, (d_1 * d_2) * K \Big)$

by Def of G group

$= \Big(d_1 * H, d_1 * K\Big) \Delta_3 \Big(d_2 * H, d_2 * K\Big)$

$= f(d_1) \Delta_3 f(d_2)$ $\Rightarrow$ Homorphisim. (1)

- Now since $|D| = \left|\frac{D}{H} \oplus \frac{D}{K}\right|$

by (ii) $|D| = |H * K| = \frac{|H||K|}{1} = \left|\frac{D}{K}\right|\left|\frac{D}{H}\right| = \left|\frac{D}{H} \oplus \frac{D}{K}\right|$

- <u>1-1</u> :

let $f(d_1) = f(d_2)$ for any $d_1, d_2 \in D$.

$(d_1 * H, d_1 * K) = (d_2 * H, d_2 * K)$.

Hence, $(d_1 * H = d_2 * H) * d_2^{-1} = d_2^{-1} * d_1 * H = H$

$\Rightarrow \boxed{d_2^{-1} * d_1 \in H}$

and $d_1 * K = d_2 * K$.

$\hookrightarrow d_2^{-1} * d_1 * K = K \Rightarrow \boxed{d_2^{-1} * d_1 \in K.}$

$d_2^{-1} * d_1 \in H \cap K$.

$\Rightarrow H \cap K = \{e\} \Rightarrow d_2^{-1} * d_1 = e \Rightarrow \boxed{d_1 = d_2}$

Hence f is 1-1 --- (2)

$\Rightarrow$ (1) and (2) $D \approx \frac{D}{H} \oplus \frac{D}{K}$.

c) Now to finish up the proof.

by part c we know $D \approx \frac{D}{H} \oplus \frac{D}{K}$

by part(a) $\Rightarrow K \approx \frac{D}{H}$

by part(b) $\Rightarrow \frac{D}{K} \approx H$.

Hence by a,b $\Rightarrow \frac{D}{H} \oplus \frac{D}{K} \approx K \oplus H$

by (c) $\Rightarrow D \approx \frac{D}{H} \oplus \frac{D}{K} \approx K \oplus H$ ∎

iv) Let H, K be subgroups of a group D. In general, $H*K$ need not be a subgroup of D. However, if K is a normal subgroup of D, then prove that $K*H$ is a subgroup of D.

Want: show $a^{-1}*b \in K*H$ for every $a, b \in K*H$.

by Def of (ii)

$K*H = \{ k*h \mid k \in K \text{ and } h \in H \}$

Now, Let a,b any elements in $K*H$, Hence they should be of the form:

$a = k_1 * h_1$ where $k_1, k_2 \in K$ and

$b = k_2 * h_2$ $h_1, h_2 \in H$

$\Rightarrow a, b \in K*H$.

Now,

we want to show $a^{-1}*b = (k_1*h_1)^{-1} * k_2 * h_2 \in K*H$.

$= h_1^{-1} * k_1^{-1} * k_2 * h_2 \in K*H$.

since K is normal, we know by class Thm.

From Lecture trick

$h_1^{-1} * \underbrace{k_1^{-1} * k_2}_{=k_3 \in K} * h_2 = k_1^{-1} * k_2 = k_3 \in K$.

$a^{-1}*b = \underbrace{(h_1^{-1} * k_3 * h_1)}_{k_3 * h} * \underbrace{h_1^{-1} * h_2}_{h \in H} = k_3 * h \in K*H$ ∎

for some $h \in H$.

(V) Let D be a group with 38 elements, K, H are subgroups of D. such that $|K| = 19$ and $|H| = 2$ s.t H is a normal subgroup of D. Prove that $D \approx \mathbb{Z}_{38}$.

D is finite, we need to show D is cyclic.

$|D/K| = 2$ ← prime so, cyclic.

$D/K = \{$ the set of all distinct left cosets $\}$.

$= \{K, a*K\}$ for $\forall$ $a \in D$. and $a \notin K$.

this also means we have 2 distinct right cosets

$= \{K, K*a\}$ for $a \in D$ and $a \notin K$.

So, $\forall b \in D$ → if $b \in K \Rightarrow b*K = K = K*b$.

→ if $b \notin D \Rightarrow b*K = D - K = a*K$ ↙ since only two distinct left coset and right

$= K*a$

$= K*b$. ← here $b = a$.

$\Rightarrow$ Hence $K \trianglelefteq D$.

Now since H, K are normal.

by (ii) and $|K| = 19$, $|H| = 2$

$\Rightarrow |D| = |H*K| = \dfrac{|H|\,|K|}{|H \cap K|} = \dfrac{19 \times 2}{\bigcirc} = 38$.

$\Rightarrow |H \cap K| = 1$. → where $H \cap K = \{e\}$

since subgroup by previous H.w.

Now, using (iii)(C)

$D \approx H \oplus K$. where H, K are cyclic since
$\approx \mathbb{Z}_2 \oplus \mathbb{Z}_{19}$ $|H| = 2$ prime ; $|K| = 19$ ~ prime

By H.W ② since by class Thm, and both are finite.
$\gcd(19, 2) = 1$

$\Rightarrow$ $H \oplus K$ is cyclic and $\boxed{D \text{ is cyclic}}$

Thus, by class-Thm. Since D is finite cyclic with 38 elements

then $D \approx \mathbb{Z}_{38}$ ∎

vi) Let D be an infinite cyclic group. Prove that D has exactly two generators.

Since D is infinite and cyclic, then by class thm, $D \approx \mathbb{Z}$.

we know $\mathbb{Z}$ is generated by $1, -1$. By the def a generator $1, -1$ only can generate $\mathbb{Z}$,
and since $D \approx \mathbb{Z}$, then D has exactly two generators.

vii) Let $U(n) = \{a \in \mathbb{Z}_n \mid \gcd(a,n) = 1\}$. Prove that $U(n)$ is a group under multiplication mod n with $\phi(n)$ elements.

- first lets show $|U(n)| = \phi(n)$.

$|U(n)| \Rightarrow$ # of elements $a \in \mathbb{Z}_n$ s.t $\gcd(a,n) = 1$.

we know $\mathbb{Z}_n = \{\underset{\downarrow n}{0}, 1, 2, \ldots, n-1\}$

So, $a \in U(n)$ that are $1 \leq a \leq n$ s.t relatively prime with n,

$\Rightarrow$ Hence, by Def. of $\phi(n) \Rightarrow$ # of such $a = \phi(n)$.

where $\phi(n)$ = # of all numbers between 1 and n that are relatively prime with n.

$\Rightarrow |U(n)| = \phi(n)$.

- closure:

Let $x, y \in U(n)$

$\Rightarrow \gcd(x,n) = 1$ and $\gcd(y,n) = 1$.

by Number Theory Facts:

$(ax + by = 1) \cdot y$ for some $a, b, c, d \in \mathbb{Z}^{+ve.}$

$(cy + dn = 1) \cdot x$.

$\Rightarrow$ $axy + byn = y$ $\Rightarrow cx[axy + byn] + dxn = x$.

in $cxy + dxn = x$ $\cancel{x}[\underbrace{cax}_{r \in \mathbb{Z}^+}y + cbyn + dn] = \cancel{x}$.

$\Rightarrow rxy + \underbrace{(bcy + d)}_{s}n = 1$.

for some $r, s \in \mathbb{Z}^+$

$\Rightarrow \boxed{rxy + sn = 1}$

Thus, $\gcd(xy, n) = 1$, and $xy \in \mathbb{Z}_n$ since $x, y \in \mathbb{Z}_n$ mod n

$\Rightarrow$ Hence $\boxed{xy \in U(n)}$ □

② <u>inverse</u>:

Let $a \in U(n)$ and since $\gcd(a,n)=1$ $\quad n \in \mathbb{Z}^+$

$\Rightarrow$ by Euler Fermat Result,

$$n \mid a^{\phi(n)} - 1$$

$$nk = a^{\phi(n)} - 1 \qquad \text{some } k \in \mathbb{Z}^+$$

$$\Rightarrow a^{\phi(n)} = nk + 1 \qquad \text{where we know } \phi(n) \in \mathbb{Z}^+$$

which means.

$$a^{\phi(n)} = 1 \mod n.$$

$\rightarrow$ identity under multiplication.

So, $\quad a \cdot a^{(\phi(n)-1)} = 1 \mod(n).$

Hence, $\quad a^{-1} = a^{(\phi(n)-1)} \mod(n).$

where $a^{\overbrace{\phi(n)-1}^{=m}}$ is just a^m some $m \in \mathbb{Z}^+$

and since we know $\gcd(a,n)=1 \rightarrow$ by previous closure part.

$$\Rightarrow \gcd(a^m, n) = 1 \Rightarrow \gcd(a^{\phi(n)-1}, n) = 1$$

$$\Rightarrow a^{\phi(n)-1} \in U(n)$$

Hence,

$$\forall a \in U(n), \ \exists a^{-1} = a^{\phi(n)-1} \in U(n) \ \blacksquare$$

③ <u>Identity</u>:

<u>want</u> $\forall a \in U(n) \cdot \exists e \in U(n)$ s.t

$$a \cdot e = e \cdot a = a \quad \mod(n).$$

Hence, $e = 1 \mod(n)$ where $\gcd(1,n)=1$

$$\text{So, } e = 1 \in U(n) \ \square$$

• Associative property:

let $a,b,c \in U(n)$

Now,

$a\cdot(b\cdot c) = (a\cdot b)\cdot c \mod n$

multiplication mod n is Associative.

Hence, By ① to ④ $\Rightarrow U(n)$ is a group. □

(ix) Prove that $U(n), n \geq 3$ is cyclic if and only if $n=4$ or $n=p^k$ or $n=2p^k$ for some ODD prime p and $k \geq 1$

$\Rightarrow$) ① • Prove $U(n)$, $n \geq 3$ is cyclic if $n=4=2^2$ $P_1 = 2$, $\alpha_1 = 2$

by (viii)

$$|U(4)| = \phi(4)$$
$$= (2-1)(2)^1 = 2.$$

Hence, by class notes since $|U(4)| = 2$ (prime)

then, $U(4)$ is cyclic.

② • Prove $U(n)$ is cyclic if $n=p^k$ where p is an ODD prime, $k \geq 1$.

$$\Rightarrow n = p^k = \underbrace{\overset{odd}{p}\cdot \overset{odd}{p}\cdot \overset{odd}{p} \cdots \overset{odd}{p}}_{k \text{ times}} \Rightarrow n \text{ is odd}$$

So, by (VII)

$$U(\overset{odd}{n}) \approx \underset{even}{Z_{p-1}} \oplus Z_{p^{k-1}} \rightarrow \text{odd} \quad \text{where } k-1 = m \in Z^+$$

Now using the Hint:

$\gcd(p-1, p) = 1 \rightarrow p-1 < p$. ; $p-1$ is even and p is odd prime.

$\Rightarrow p-1 \nmid p$

$\Rightarrow p-1 \neq p$ because p is prime.

then for $p^m = \underbrace{p \cdot p \cdots p}_{m \text{ times}}$ for $m \in \mathbb{Z}^+$

the factors for $p^m = 1, p^i$ $1 \le i \le m$.

$\Rightarrow$ Hence, $p-1 \nmid p^m$

$\Rightarrow \gcd(p-1, p^m) = 1 \Rightarrow \gcd(p-1, p^{k-1}) = 1.$

then by H.W 2

$\mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^{k-1}}$ is cyclic

and thus,

$U(n)$ is cyclic since isomorphic to $\mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^{k-1}}$

3 • Prove $U(n)$ is cyclic if $n = 2p^k$ (p is odd prime)

$$n = \underbrace{\underset{\substack{\downarrow \\ \text{prime} \\ \text{even}}}{2} \cdot \underset{\text{odd}}{p^k}}_{\text{even}}$$

$\Rightarrow n$ is even.

Sine p is odd prime it will be > 2 so, $p_1 < p_2 = p$.

then by (Viii) since $\alpha_1 = 1$

$\Rightarrow U(n) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^{k-1}}$

where $\gcd(p-1, p^{k-1}) = 1$ as proved above.

then by H.W result, $\mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^{k-1}}$ is cyclic.

$\Rightarrow U(n)$ is cyclic

[Hene, by 1, 2 and 3, $U(n)$ is cyclic for $n \geq 3$ iff $n = 4$ or $n = p^k$ or $n = 2p^k$ where $k \geq 1$.]

$\Leftarrow$ if $U(n)$ is cyclic prove that $n=4$ or $n=p^k$ or $n=2p^k$ for $k\geq 1$.

Now if we study the cases of n,

$n =$ odd → prime → $n=p$ for some p odd, prime

odd → $\boxed{\text{not prime.}}$ (Case 1) → $n = p_1 p_2 p_3 \cdots p_k$. X ; $n = p^k$. ✓

even → 2 → $U(2)=\{1\}$ → trivial.

even → $\boxed{\text{not prime}}$ (Case 2) → $n=2^{\alpha_1}p^k$ ✓ if $\alpha_1 = 1$; $n = 2^{\alpha_1}$ ✓ if $\alpha_1 = 1$ or 2 ; $n = 2^{\alpha_1} p_1 p_2 \cdots p_k$ X.

- first notice if $n=p$.

then $U(n) \approx \mathbb{Z}_{p-1} \Rightarrow \mathbb{Z}_{p-1}$ is cyclic.

implies $U(n)$ cyclic ✓ as assumed. --(*)

Now, it remains to study case 1 and Case 2;

Case 1: $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$ (can b written as) for some $k\in\mathbb{Z}^+$.

where $p_1, p_2, p_3 \cdots p_k$ are odd prime numbers.

Assume $p_i \neq p_j$ for $1\leq i\neq j\leq k$, hence distinct p_i, p_j

W.L.O.G:

Let $n = p_1^{\alpha_1}\cdot p_2^{\alpha_2}$. where $p_1 \neq p_2$, p_1 and p_2 are odd primes and $p_1 < p_2$.

Then by (viii), "odd"

$$U(n) \approx \underbrace{\mathbb{Z}_{p_1-1} \oplus \mathbb{Z}_{p_1^{\alpha_1-1}}}_{\gcd(p_1-1,\, p_1^{\alpha_1}-1)=1} \oplus \underbrace{\mathbb{Z}_{p_2-1} \oplus \mathbb{Z}_{p_2^{\alpha_2-1}}}_{\gcd(p_2-1,\, p_2^{\alpha_2-1})=1}$$

↓ cyclic ↓ cyclic

$$\gcd[\underbrace{\underbrace{(p_1-1)}_{\text{even}}\underbrace{(p_1^{\alpha_1-1})}_{\text{odd}}}_{\text{even}} ; \underbrace{\underbrace{(p_2-1)}_{\text{even}}\underbrace{(p_2^{\alpha_2-1})}_{\text{odd}}}_{\text{even}}]$$

and the $\gcd(\text{even}, \text{even}) \neq 1$.

Since $(p_1 - 1)(p_1^{\alpha_1 - 1})$ and $(p_2 - 1)(p_2^{\alpha_2 - 1})$ are even.

Hence, $U(n)$ is Not cyclic Contradiction.

as, $\mathbb{Z}_{p_1 - 1} \oplus \mathbb{Z}_{p^{\alpha_1 - 1}} \oplus \mathbb{Z}_{p_2 - 1} \cdots$ is Not cyclic.

by previous H.W problem.

$\Rightarrow$ Note that this can be generated to any k prime odd numbers $\Rightarrow$ $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

(a) Thus, $p_i = p_j$ can't be distinct for $\forall\ 1 \leq i \neq j \leq k$.

Hence, $n = p^k$ for $k \geq 2$ and by $(*)$ $\Rightarrow$ $\boxed{n = p^k \ \forall\ k \geq 1}$

when $U(n)$ is cyclic and p are odd prime numbers

Now, Case 2:

where n is even, we know that any even number n can be written in the prime factorization as

$n = 2^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ or it can be $\boxed{n = 2^{\alpha_1}} \rightarrow (**)$.

where 2 is the only even prime number so, $p_2, p_3, \cdots p_k$ are odd prime numbers., then by case (1) we know, p_i, p_j can't be distinct where $1 \leq i \neq j \leq k$, for the same reason as in case (1).

Hence, $n = 2^{\alpha_1} p^k \quad k \geq 1.,\ \alpha_1 \geq 1$

Now, Lets assume that $\alpha_1 > 1$ and $n = 2^{\alpha_1} p^k$

so, n (even), Hence by (Viii)

$$U(n) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{\alpha_1 - 2}} \oplus \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^{k-1}}$$

clearly $\gcd(2, 2^{\alpha_1 - 2}) \neq 1$, so $U(n)$ is Not cyclic.

since by H.w result $\mathbb{Z}_2 \oplus \mathbb{Z}_{2^{\alpha_1-2}}$ is Not cyclic.

Also if $\boxed{\alpha_1 = 2}$ $\Rightarrow \gcd(2, p-1) \neq 1$ since $p-1$ is even,

But, according to the Hint in (Vii) $\mathbb{Z}_2 \oplus \mathbb{Z}_{2^{\alpha_1-2}}$ part will be removed $\boxed{\text{if } \alpha_1 = 1}$

so,

$$\Rightarrow U(n) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^{k-1}}$$

where as proved earlier in this question

$\gcd(p-1, p^{k-1}) = 1 \Leftrightarrow \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^{k-1}}$ is cyclic $\Leftrightarrow U(n)$ is cyclic.

$\Rightarrow$ Thus, if $U(n)$ is cyclic, $n = 2p^k$ for p odd prime odd number and $k \geq 1$. (b)

- Now, we treat the last possible case, where.

as in (**) $n = \underbrace{2^{\alpha_1}}_{\text{even}}$, $\alpha_1 \geq 1$.

$$U(n) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{\alpha_1 - 2}}$$

$\rightarrow \gcd(2, 2^{\alpha_1 - 2}) = 2 \neq 1$

Hence contradiction

$U(n)$ Not cyclic.

so, $\alpha_1 = 1$ or $\alpha_1 = 2$

$\alpha_1 = 1 \downarrow$ trivial

$\alpha_1 = 2 \Downarrow$ $n = 2^2 = 4$

$U(4) \approx \mathbb{Z}_2 \Rightarrow$ $U(4)$ is cyclic as $\mathbb{Z}_2$ is cyclic (c)

Hence, by (a), (b), (c) $\Rightarrow$ If $U(n)$ is cyclic then $n=4$ or $n=p^k$ or $n=2p^k$ $k \geq 1$ and p odd prime.

and by the two results in green.

$\Rightarrow$ $U(n)$, $n \geq 3$ is cyclic iff $n=4$ or $n=p^k$ or $n=2p^k$ for some ODD prime p and $k>1$.

(x) Prove that $U(64)$ has an element of order 16 but it has no elements of order 32.

$n = 64 = 2 \cdot 32 = 2 \cdot 2 \cdot 16 = \boxed{2^6}$

$|U(64)| = \phi(64)$
$= (2-1)\, 2^{6-1}$
$= 2^5 = 32 < \infty$ So, by class notes.

for $\forall a \in U(64) \Rightarrow |a| \mid 32$

Then, $|a| = 1, 32, 2, 16, 4, 8,$ —— ①

but since $n = 2^5$ where $n \neq 4$ and $n \neq p^k$ and $n \neq 2p^k$.
2 even — odd prime p.

Hence, $U(64)$ is Not cyclic by (ix)

then by class notes since $|U(64)| < \infty$, $\nexists\, a \in U(64)$ s.t $|a| = 32$. (No element with order 32).

Now by (viii)

$U(64) \approx Z_2 \oplus Z_{2^4}$
$\approx Z_2 \oplus Z_{16}$

$a \in Z_2$ and $b \in Z_{16}$

then by previous H.W $|(a,b)| = LCM(|a|, |b|)$ $\forall (a,b) \in Z_2 \oplus Z_{16}$.

take the generators of Z_2 and Z_{16} (to find the Max element's order)

$|(1,1)| = \dfrac{|1|\,|1|}{\gcd(2,16)}$

$= \dfrac{2 \cdot 16}{2} = 16.$

Hence, $\forall a \in U(64) \Rightarrow |a| \leq 16$, so $U(64)$ has an element of order 16 but Not 32.

16

Scanned with CamScanner

(xi) Prove that $D = (\mathbb{Z}_5, +) \oplus U(18)$ is cyclic and Hence. $D \approx (\mathbb{Z}_m, +)$ find m.

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, $\mathbb{Z}_{18} = \{0, 1, 2, \ldots, 17\}$

$U(18) = \{a \in \mathbb{Z}_{18} \mid \gcd(a, 18) = 1\}$

$= \{1, 5, 7, 11, 13, 17\}$.

to check:

$\phi(18) = (2-1).2^{1-1} \cdot (3-1)\, 3^{1}$

$= 2 \cdot 3 = \boxed{6}$

proof:

$\Rightarrow n = 18 = 2 \cdot 3^2$, we notice it is of the form $2p^k$.
where $p = 3$ odd prime, Hence by (ix) U(18) is cyclic

Also,

$|D| = |\mathbb{Z}_5| \, |U(18)|$

$= 5 \cdot 6 = 30 < \infty$.

Now, by class Thm D is a finite, cyclic group with 30 elements so, $\Rightarrow D \approx (\mathbb{Z}_{30}, +) \Rightarrow \boxed{m = 30}$

(xii) Prove that $(\mathbb{Q}^*, \cdot)$ is not cyclic.

Assume by contradiction that $\mathbb{Q}^*$ is cyclic, and since it is infinite group, then by Class thm.

for $\forall\, q \in \mathbb{Q}^* / \{e\} \rightarrow |q| = \infty$.

but $\exists\, -1 \in \mathbb{Q}^*$ and $-1 \neq e = 1$

where $|-1| = 2 < \infty$ contradiction!

2.2.8 Solution for HW-Five

Farah Zeyad   HW 5

900086476

1) Let D be an abelian group with $2^3 5^2$ elements

i) Suppose that D has exactly one subgroup with 4 elements.

Find all non-isomorphic group with these properties.

Solution:

All non-isomorphic group without the condition

$$\begin{matrix} 3 & & 2 \\ 1+2 & & 1+1 \\ 1+1+1 & & \end{matrix}$$

we have

① $\mathbb{Z}_8 \oplus \mathbb{Z}_{25}$, ② $\mathbb{Z}_8 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, ③ $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{25}$

④ $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$ ⑤ $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{25}$ ⑥ $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$

Now suppose D has exactly one subgroup with 4 element:

Then we have to check which one of them has exactly one subgrop with 4 elements by using "obsevation"

① $D = \mathbb{Z}_8 \oplus \mathbb{Z}_{25}$: let H be a subgroup of $\mathbb{Z}_8$ with order 4

$\Rightarrow$ $H \oplus \{0\}$ is the only subgrup with order 4

② $D = \mathbb{Z}_8 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$: Same of $\mathbb{Z}_8 \oplus \mathbb{Z}_{25}$, $H + \{0\} + \{0\}$ The only subgroup of order 4

③ $D = \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{25}$: let K be a subgroup of $\mathbb{Z}_4$ with 2 elements

$\Rightarrow$ $\mathbb{Z}_2 \oplus K \oplus \{0\}$ and $\{0\} + \mathbb{Z}_4 \oplus \{0\}$ are two subgroup with 4 elements but D has exactly one subgroup of orde 4 contradiction

④ $D = \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$: same of ③ because $\mathbb{Z}_2 \oplus K \oplus \{0\} + \{0\}$ and $\{0\} \oplus \mathbb{Z}_4 \oplus \{0\} + \{0\}$ are two subgroup with order 4. Contradiction

$\Leftarrow$

(5) $D = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{25}$: it has three subgroup of order 4

$F = \mathbb{Z}_2 \oplus \{0\} \oplus \mathbb{Z}_2 \oplus \{0\}$ and $W = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \{0\} \oplus \{0\}$

and $L = \{0\} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \{0\}$ like $|(1,0,1,0)| = |(1,1,0,0)| = |(0,1,1,0)|$

$= 4$ Contradiction

(6) $D = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$: same as (5) has three element of order 4. Contradiction

Therefore The all non-isomorphic group with this properties are:

$\mathbb{Z}_8 \oplus \mathbb{Z}_{25}$ and $\mathbb{Z}_8 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$

ii) Suppose that D has exactly one subgroup with 4 elements and it has exactly one subgroup with 5 elements. Find all non-isomorphic group with these properties.

From (i) we have only two group that has one subgroup of order 4 :

$D = \mathbb{Z}_8 \oplus \mathbb{Z}_{25}$ and $D = \mathbb{Z}_8 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$

Now check if they have alse one subgroup of order 5

(1) $D = \mathbb{Z}_8 \oplus \mathbb{Z}_{25}$: Let H be a subgroup of $\mathbb{Z}_{25}$ with 5 elements

Then $\{0\} + H$ is the only subgroup of order 5.

$\Rightarrow$ D has one subgroup of order 5

(2) $D = \mathbb{Z}_8 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$: this group has two subgroup of order 5

$\{0\} \oplus \mathbb{Z}_5 \oplus \{0\}$ and $\{0\} \oplus \{0\} \oplus \mathbb{Z}_5$

$\Rightarrow$ D has two subgroup of order 5 Contradiction

$\Rightarrow$ $\mathbb{Z}_8 \oplus \mathbb{Z}_{25}$ are the only group that has one subgroup of order 4 and one subgroup of order 5.

2| Let D be a cyclic group with 100 elements. Convince me that $(Aut(D), \circ)$ is abelian group and find $m_1, \dots, m_k$ such that

$Aut(D) \approx \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_k}$

Solution :-

Since D is finite cyclic group with 100 element

$\Rightarrow D \approx \mathbb{Z}_{100}$

$\Rightarrow (Aut(D), \circ) \approx (Aut(\mathbb{Z}_{100}), \circ)$

from Lecture notes we know $\forall n \geq 2 \; (Aut(\mathbb{Z}_n), \circ) \approx (U(n), \cdot)$

$\Rightarrow (Aut(\mathbb{Z}_{100}), \circ) \approx (U(100), \cdot)$

From HW 4:- $U(100)$ is a group under multiplication mod 100

$\Rightarrow U(100) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5$ since $gcd(4,5) = 1$

$U(100) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{20}$ $\Rightarrow$ Since $\mathbb{Z}_2 \oplus \mathbb{Z}_{20}$ is abelian

$\Rightarrow U(100)$ is abelian group.

$\Rightarrow$ Since $Aut(\mathbb{Z}_{100}) \approx U(100)$

$\Rightarrow (Aut(\mathbb{Z}_{100}), \circ)$ is abelian group

$\Rightarrow (Aut(D), \circ)$ is abelian group

From HW 4:

$Aut(D) \approx Aut(\mathbb{Z}_{100}) \approx U(100) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5$

$\Rightarrow Aut(D) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5$

case1 $\Rightarrow m_1 = 2, \; m_2 = 4, \; m_3 = 5$

but also since $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{20}$ since $gcd(4,5) = 1$

$\Rightarrow Aut(D) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{20}$

case 2 $\Rightarrow m_1 = 2, \; m_2 = 20$

3| Prove that every group with $n = 17 \times 3^2$ is abelian. Find all non-isomorphic group with n elements

Solution:- $|D| = 153 = 17 \times 3^2$ prove D is abelian

n_3 = # of all Sylow-3-subgroup

$\Rightarrow n_3 \Big| \frac{|D|}{|Syl(3)|} = n_3 \Big| 17 \Rightarrow n_3 = 1$ or 17

$\Rightarrow 3 \mid n_3 - 1 \Rightarrow 3 \mid (1-1) \Rightarrow 3 \mid 0$ ✓ but $3 \nmid 17-1 \Rightarrow 3 \nmid 16$

$\Rightarrow n_3 = 1 \Rightarrow D$ has exactly one sylow-3-subgroup say H

Since $n_3 = 1 \Rightarrow H \trianglelefteq D \Rightarrow |H| = 3^2 = 9$

n_{17} = # of all Sylow-17-Subgroup

$\Rightarrow n_{17} \Big| \frac{|D|}{|Syl(17)|} \Rightarrow n_{17} \mid 3^2 \Rightarrow n_{17} = 1$ or 3 or 9

$\Rightarrow 17 \mid n_{17} - 1 \Rightarrow$ if $n_{17} = 1 \Rightarrow 17 \mid (1-1) \Rightarrow 17 \mid 0$ ✓

if $n_{17} = 3 \Rightarrow 17 \nmid (3-1) \Rightarrow 17 \nmid 2$ ✗

if $n_7 = 9 \Rightarrow 17 \nmid (9-1) \Rightarrow 17 \nmid 8$ ✗

$\Rightarrow n_{17} = 1 \Rightarrow D$ has exactly one sylow-17-subgroup say K

since $n_{17} = 1 \Rightarrow K \trianglelefteq D. \Rightarrow |K| = 17$

Since $H, K \trianglelefteq D$ and $H \cap K = \{e\} \Rightarrow |HK| = \frac{|H||K|}{|H \cap K|} = \frac{9 \times 17}{1} = 153$

$\Rightarrow HK = D \Rightarrow D \approx H \oplus K$

Since $|K| = 17 \Rightarrow K \approx \mathbb{Z}_{17}$ and $|H| = 3^2 = 9$ since

H is abelian subgroup of D $H \approx \mathbb{Z}_9$ or $H \approx \mathbb{Z}_3 \oplus \mathbb{Z}_3$

$\Rightarrow D \approx \mathbb{Z}_9 \oplus \mathbb{Z}_{17}$ since $\gcd(9,17) = 1 \Rightarrow D$ is cyclic

$\Rightarrow$ D is abelian

$\Rightarrow$ and $D \approx \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{17} \Rightarrow$ Not Cyclic but since $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ and $\mathbb{Z}_{17}$ is abelian $\Rightarrow$ D is abelian

$\Rightarrow$ D is abelian and $\mathbb{Z}_9 \oplus \mathbb{Z}_{17}$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{17}$ are the all Non-isomorphic group with $n = 153$ elements

4) Let D be a group with 5 · 11 · 29. prove that D has exactly one subgroup with 29 elements, say H and $H \subseteq C(D)$.

Solution :-

prove that D has one subgroup of order 29

So by Sylow theorem:

n_{29} = # of all sylow - 29 - subgroup

$n_{29} \mid \frac{|D|}{|Syl(29)|} \Rightarrow n_{29} \mid 5 \times 11 \Rightarrow n_{29} = 1, 5, 11, 55$

$\Rightarrow 29 \mid n_{29} - 1 \Rightarrow$ if $n_{29} = 1 \Rightarrow 29 \mid (1-1) \Rightarrow 29 \mid 0$ ✓

if $n_{29} = 5 \Rightarrow 29 \nmid (5-1) \Rightarrow 29 \nmid 4$ ×

if $n_{29} = 11 \Rightarrow 29 \nmid (11-1) \Rightarrow 29 \nmid 10$ ×

if $n_{29} = 55 \Rightarrow 29 \nmid (55-1) \Rightarrow 29 \nmid 54$ ×

$\Rightarrow n_{29} = 1$

$\Rightarrow$ D has exactly one sylow - 29 - subgroup say H

let H be sylow - 29 - subgroup $\Rightarrow H \triangleleft D$

Since $H \triangleleft D$ we conclude $D/C(H) \approx$ subgroup of $Aut(H)$

Since $|H| = 29$, H is cyclic $\Rightarrow H \approx \mathbb{Z}_{29}$

$\Rightarrow D/C(H) \approx$ subgroup of $Aut(\mathbb{Z}_{29}) \approx U(29)$

$\Rightarrow \left| D/C(H) \right| \Big| \, |D|$ and $\left| D/C(H) \right| \Big| \, |U(29)| = 28$

$\Rightarrow gcd(28, 1595) = 1 \Rightarrow \left| D/C(H) \right| = 1$

$\Rightarrow H \subseteq C(D)$.

5] let D be a group with 216 elements. prove that D is Not Simple

Solution :

let D be a group where $|D| = 216 = 2^3 \cdot 3^3$

$n_3 = \#$ of all sylow-3-subgroup

$n_3 \mid \frac{|D|}{|Syl(3)|} = 2^3 \Rightarrow n_3 \mid 2^3 \Rightarrow n_3 = 1, 2, 4, 8$

$3 \mid (n_3 - 1) \Rightarrow$ if $n_3 = 1 \Rightarrow 3 \mid (1-1) \Rightarrow 3 \mid 0$ ✓

if $n_3 = 2 \Rightarrow 3 \mid (2-1) \Rightarrow 3 \nmid 1$ ×

if $n_3 = 4 \Rightarrow 3 \mid (4-1) \Rightarrow 3 \mid 3$ ✓

if $n_3 = 8 \Rightarrow 3 \mid (8-1) \Rightarrow 3 \nmid 7$ ×

$\Rightarrow n_3 = 1$ or 4

$n_2 = \#$ of all sylow-2-subgroup

$n_2 \mid \frac{|D|}{|Syl(2)|} \Rightarrow n_2 \mid 3^3 \Rightarrow n_2 = 1, 3, 9, 27$

$\Rightarrow 2 \mid (n_2 - 1) \Rightarrow$ if $n_2 = 1 \Rightarrow 2 \mid (1-1) \Rightarrow 2 \mid 0$ ✓

if $n_2 = 3 \Rightarrow 2 \mid (3-1) \Rightarrow 2 \mid 2$ ✓

if $n_2 = 9 \Rightarrow 2 \mid (9-1) \Rightarrow 2 \mid 8$ ✓

if $n_2 = 27 \Rightarrow 2 \mid 27-1 \Rightarrow 2 \mid 26$ ✓

$\Rightarrow n_2 = 1, 3, 9, 27$

Since $n_3 = 1$ or $n_3 = 4 \Rightarrow$ Assume $n_3 \neq 1$, $n_2 \neq 1$

let $n_3 = 4$ $\exists$ a group homorphisim $K: D \longrightarrow S_4$ s.t

$\frac{D}{Ker(K)} \cong$ subgroup of S_4 and $Ker(K) \neq D$ $[Ker(K) \triangleleft D]$

we want to show $Ker(K) \neq \{e\} \Rightarrow$ Deny Assume $Ker(K) = \{e\}$

$\Rightarrow D \cong$ Subgroup of S_4 but since $|D| = 216$ and

$|S_4| = 4! = 24$ impossible Contradiction

$\Rightarrow Ker(K) \neq \{e\} \Rightarrow D$ is Not Simple.

6] Let D be a group with $5 \cdot 7 \cdot 17$ elements. prove that D is not Simple. Assume that $n_{17} \neq 1$. How many element in D have order 17.?

Solution

let D be a group with $5 \times 7 \times 17 = 595$ elements

Prove D is not Simple.

n_5 = # of all sylow - 5 - Subgroup

$\Rightarrow n_5 \Big| \frac{|D|}{|Syl(5)|} \Rightarrow n_5 \big| 7 \times 17 \Rightarrow n_5 = 1, 7, 17, 119$

$\Rightarrow 5 \big| (n_5 - 1) \Rightarrow$ if $n_5 = 1 \Rightarrow 5 \mid (1-1) \Rightarrow 5 \mid 0$ ✓

if $n_5 = 7 \Rightarrow 5 \nmid (7-1) \Rightarrow 5 \nmid 6$ ✗

if $n_5 = 17 \Rightarrow 5 \nmid (17-1) \Rightarrow 5 \nmid 16$ ✗

if $n_5 = 119 \Rightarrow 5 \nmid (119-1) \Rightarrow 5 \nmid 118$ ✗

$\Rightarrow n_5 = 1 \Rightarrow$ D has exactly one Sylow - 5 - Subgroup

$\Rightarrow$ Let H is the sylow - 5 - subgroup $\Rightarrow H \lhd D$

$\Rightarrow$ There fore D. is Not Simple.

n_{17} = # of all sylow - 17 - subgroup

$n_{17} \Big| \frac{|D|}{|Syl(17)|} \Rightarrow n_{17} \big| 5 \times 7 \Rightarrow n_{17} = 1, 5, 7, 35$

$\Rightarrow 17 \big| (n_{17} - 1) \Rightarrow$ if $n_{17} = 1 \Rightarrow 17 \mid (1-1) \Rightarrow 17 \mid 0$ ✓

if $n_{17} = 5 \Rightarrow 17 \nmid (5-1) \Rightarrow 17 \nmid 4$ ✗

if $n_{17} = 7 \Rightarrow 17 \nmid (7-1) \Rightarrow 17 \nmid 6$ ✗

if $n_{17} = 35 \Rightarrow 17 \mid (35-1) \Rightarrow 17 \mid 34$ ✓

$\Rightarrow n_{17} = 1$ or $n_{17} = 35$

Assume $n_{17} \neq 1 \Rightarrow$ There are 35 Sylow - 17 - Subgroup

but $|e| = 1 \Rightarrow$ So we have only 16 element of order 17

So the 35 Sylow - 17 - Subgroup have

$35 \times 16 = 560$ element of order 17.

2.2.9 Solution for HW-Six

Farah Zeyad HW6
900086476

Question 1 i): Let $B=\begin{bmatrix} \{1,2\} & \{2,4\} \\ \{3,4\} & \{1,4\} \end{bmatrix}$. Does B^{-1} exists? if yes then find it. If no then explain

Solution

1) check if $|B| \in U(A) \Rightarrow |B| = F$, so by finding deterimant of B we have.

$\Rightarrow |B| = \{1,2\}\cdot\{1,4\} + -\{2,4\}\{1,4\}$ Note $-\{2,4\} = \{2,4\}$

$= \{1,2\}\{1,4\} + \{2,4\}\{1,4\}$

$= \{1,2\} \cap \{1,4\} + \{2,4\} \cap \{1,4\}$

$\{1\} + \{4\} = \{1\} - \{4\} \cup \{4\} - \{1\} = \{1,4\}$

$\Rightarrow |B| = \{1,4\}$

No, B^{-1} Does not exist because B is invertible if and only if $|B| \in U(A)$ where $U(A) = \{F\}$, since $|B| = \{1,4\} \neq F \Rightarrow |B| \notin U(A)$

There Fore B is not invertible has no inverse $\Rightarrow B^{-1}$ Does not exist.

ii) Let $B=\begin{bmatrix} \{2,3\} & \{1,3,4\} \\ \{1,3,4\} & \{2,4\} \end{bmatrix}$ Does B^{-1} exist? if yes then find it. If no then explain.

Solution

1) check if $|B| \in U(A) \Rightarrow |B| = F$ so by finding the determinat we have.

$|B| = \{2,3\}\{2,4\} + -\{1,3,4\}\{1,3,4\}$ Note $-\{1,3,4\} = \{1,3,4\}$

$= \{2,3\} \cap \{2,4\} + \{1,3,4\} \cap \{1,3,4\}$

$\{2\} + \{1,3,4\}$

$= \{2\} - \{1,3,4\} \cup \{1,3,4\} - \{2\}$

$= \{2\} \cup \{1,3,4\}$

$= \{1,2,3,4\}$

$\Rightarrow |B| = \{1,2,3,4\} = F$

$\Rightarrow |B| \in U(A) = \{F\}$

yes, B^{-1} exist since $|B| = F$. Now find B^{-1}

$$\Rightarrow B^{-1} = \frac{F}{F}\begin{bmatrix}\{2,4\} & \{1,3,4\}\\ \{1,3,4\} & \{2,3\}\end{bmatrix} = F\begin{bmatrix}\{2,4\} & \{1,3,4\}\\ \{1,3,4\} & \{2,3\}\end{bmatrix}$$

$$\Rightarrow B^{-1} = \begin{bmatrix}\{2,4\} & \{1,3,4\}\\ \{1,3,4\} & \{2,3\}\end{bmatrix}$$

Check if $BB^{-1} = \begin{bmatrix}F & \emptyset\\ \emptyset & F\end{bmatrix} = B^{-1}B$ Note $\{3\}+\{3\}=\emptyset$

$$\Rightarrow BB^{-1} = \begin{bmatrix}\{2,3\} & \{1,3,4\}\\ \{1,3,4\} & \{2,4\}\end{bmatrix}\begin{bmatrix}\{2,4\} & \{1,3,4\}\\ \{1,3,4\} & \{2,3\}\end{bmatrix} = \begin{bmatrix}\{2\}+\{1,3,4\} & \{3\}+\{3\}\\ \{4\}+\{4\} & \{1,3,4\}+\{2\}\end{bmatrix}$$

$= \begin{bmatrix}F & \emptyset\\ \emptyset & F\end{bmatrix}$ There Fore B has inverse $B^{-1} = \begin{bmatrix}\{2,4\} & \{1,3,4\}\\ \{1,3,4\} & \{2,3\}\end{bmatrix}$

iii) Let $B = \begin{bmatrix}F & \{2,4\} & \{1\}\\ \{1,3\} & F & \{3\}\\ \{2\} & \{2\} & F\end{bmatrix}$. If possible Find B^{-1}.

Note $-\{2,4\} = \{2,4\}$

- First check if $|B| \in U(A) = F$

$$|B| = F\begin{bmatrix}F & \{3\}\\ \{2\} & F\end{bmatrix} - \{2,4\}\begin{bmatrix}\{1,3\} & \{3\}\\ \{2\} & F\end{bmatrix} + \{1\}\begin{bmatrix}\{1,3\} & F\\ \{2\} & \{2\}\end{bmatrix}$$

$= F(F\cap F + -\{2\}\cap\{3\}) + \{2,4\}(\{1,3\}\cap F + -\{2\}\cap\{3\}) + \{1\}(\{1,3\}\cap\{2\} - \{2\}\cap F)$

$= F(F+\emptyset) + \{2,4\}(\{1,3\}+\emptyset) + \{1\}(\emptyset+\{2\})$

$= F + \emptyset + \emptyset = F$

$\Rightarrow |B| = F \Rightarrow B^{-1}$ exist. Now Find B^{-1} using row operation

$$\left[\begin{array}{ccc|ccc}F & \{2,4\} & \{1\} & F & \emptyset & \emptyset\\ \{1,3\} & F & \{3\} & \emptyset & F & \emptyset\\ \{2\} & \{2\} & F & \emptyset & \emptyset & F\end{array}\right] \xrightarrow[\{2\}R_1+R_3\to R_3]{\{1,3\}R_1+R_2\to R_2} \left[\begin{array}{ccc|ccc}F & \{2,4\} & \{1\} & F & \emptyset & \emptyset\\ \emptyset & F & \{1,3\} & \{1,3\} & F & \emptyset\\ \emptyset & \emptyset & F & \{2\} & \emptyset & F\end{array}\right]$$

$$\xrightarrow{\{2,4\}R_2+R_1\to R_1} \left[\begin{array}{ccc|ccc}F & \emptyset & \{1\} & F & \{2,4\} & \emptyset\\ \emptyset & F & \{1,3\} & \{1,3\} & F & \emptyset\\ \emptyset & \emptyset & F & \{2\} & \emptyset & F\end{array}\right] \xrightarrow[\{1\}R_3+R_1\to R_1]{\{1,3\}R_3+R_2\to R_2}$$

$$\left[\begin{array}{ccc|ccc}F & \emptyset & \emptyset & F & \{2,4\} & \{1\}\\ \emptyset & F & \emptyset & \{1,3\} & F & \{1,3\}\\ \emptyset & \emptyset & F & \{2\} & \emptyset & F\end{array}\right]$$

So $B^{-1} = \begin{bmatrix} F & \{2,4\} & \{1\} \\ \{1,3\} & F & \{1,3\} \\ \{2\} & \emptyset & F \end{bmatrix}$

Now check that $BB^{-1} = \begin{bmatrix} F & \emptyset & \emptyset \\ \emptyset & F & \emptyset \\ \emptyset & \emptyset & F \end{bmatrix}$

$\Rightarrow BB^{-1} = \begin{bmatrix} F & \{2,4\} & \{1\} \\ \{1,3\} & F & \{3\} \\ \{2\} & \{2\} & F \end{bmatrix} \begin{bmatrix} F & \{2,4\} & \{1\} \\ \{1,3\} & F & \{1,3\} \\ \{2\} & \emptyset & F \end{bmatrix} = \begin{bmatrix} F & \emptyset & \emptyset \\ \emptyset & F & \emptyset \\ \emptyset & \emptyset & F \end{bmatrix}$

There Fore it's possible for B to have an inverse where $B^{-1} = \begin{bmatrix} F & \{2,4\} & \{1\} \\ \{1,3\} & F & \{1,3\} \\ \{2\} & \emptyset & F \end{bmatrix}$

Question 2: Convince me that $B=\begin{bmatrix} 2 & 5 & 4 \\ 1 & 1 & 2 \\ 3 & 3 & 5 \end{bmatrix}$ is invertible over $\mathbb{Z}_8$

Solution:-

* B is invertible iff $|B| \in U(\mathbb{Z}_8) = U(8)$ So Now Find the determinant of B. "$|B|$"

$$|B| = 2\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} - 5\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} + 4\begin{bmatrix} 1 & 1 \\ 3 & 3 \end{bmatrix}$$

$-5 \bmod 8 = 3$

$-1 \bmod 8 = 7$

$-2 \bmod 8 = 6$

$$2(5-6) + 3(5-6) + 4(3-3)$$

$$= 2(-1) + 3(-1) + 0$$

$$= 2(7) + 3(7) = 35 \bmod 8 = 3$$

There Fore $|B| = 3$ Since $3 \in U(\mathbb{Z}_8) = U(8)$ There Fore B is invertible.

Now Find the inverse using row operation

$$\left[\begin{array}{ccc|ccc} 2 & 5 & 4 & 1 & 0 & 0 \\ 1 & 1 & 2 & 0 & 1 & 0 \\ 3 & 3 & 5 & 0 & 0 & 1 \end{array}\right] \xrightarrow[R_1 \leftrightarrow R_2]{\text{Change } R_1 \text{ with } R_2} \left[\begin{array}{ccc|ccc} 1 & 1 & 2 & 0 & 1 & 0 \\ 2 & 5 & 4 & 1 & 0 & 0 \\ 3 & 3 & 5 & 0 & 0 & 1 \end{array}\right]$$

$$\xrightarrow{-2R_1+R_2} \left[\begin{array}{ccc|ccc} 1 & 1 & 2 & 0 & 1 & 0 \\ 0 & 3 & 0 & 1 & -2 & 0 \\ 3 & 3 & 5 & 0 & 0 & 1 \end{array}\right] \xrightarrow{-3R_1+R_3} \left[\begin{array}{ccc|ccc} 1 & 1 & 2 & 0 & 1 & 0 \\ 0 & 3 & 0 & 1 & 6 & 0 \\ 0 & 0 & -1 & 0 & -3 & 1 \end{array}\right]$$

$-3 \bmod 8 = 5$, $-1 \bmod 8 = 7$

$$\longrightarrow \left[\begin{array}{ccc|ccc} 1 & 1 & 2 & 0 & 1 & 0 \\ 0 & 3 & 0 & 1 & 6 & 0 \\ 0 & 0 & 7 & 0 & 5 & 1 \end{array}\right] \xrightarrow[\frac{1}{7}R_3]{\frac{1}{3}R_2} \left[\begin{array}{ccc|ccc} 1 & 1 & 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & \frac{1}{3} & 2 & 0 \\ 0 & 0 & 1 & 0 & \frac{5}{7} & \frac{1}{7} \end{array}\right]$$

$\frac{1}{3}$ have a meaning in $\mathbb{Z}_8$ since $3 \in U(\mathbb{Z}_8) = U(8) \Rightarrow 3^{-1} \times 1 = 3 \in \mathbb{Z}_8$

$\frac{1}{7}$ have meaning in $\mathbb{Z}_8$ since $7 \in U(\mathbb{Z}_8) = U(8) \Rightarrow 7^{-1} \times 1 = 7 \in \mathbb{Z}_8$

same For $\frac{5}{7} \Rightarrow 7 \in U(\mathbb{Z}_8) \Rightarrow 7^{-1} \times 5 = 3 \in \mathbb{Z}_8$

$$\longrightarrow \left[\begin{array}{ccc|ccc} 1 & 1 & 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 3 & 2 & 0 \\ 0 & 0 & 1 & 0 & 3 & 7 \end{array}\right] \xrightarrow{R_1 - R_2} \left[\begin{array}{ccc|ccc} 1 & 0 & 2 & -3 & -1 & 0 \\ 0 & 1 & 0 & 3 & 2 & 0 \\ 0 & 0 & 1 & 0 & 3 & 7 \end{array}\right]$$

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 2 & 5 & 7 & 0 \\ 0 & 1 & 0 & 3 & 2 & 0 \\ 0 & 0 & 1 & 0 & 3 & 7 \end{array}\right] \xrightarrow{-2R_3+R_1} \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 5 & 1 & -14 \\ 0 & 1 & 0 & 3 & 2 & 0 \\ 0 & 0 & 1 & 0 & 3 & 7 \end{array}\right]$$

$-14 \bmod 8 = 2$

$$\longrightarrow \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 5 & 1 & 2 \\ 0 & 1 & 0 & 3 & 2 & 0 \\ 0 & 0 & 1 & 0 & 3 & 7 \end{array}\right]$$

$$\Rightarrow B^{-1} = \begin{bmatrix} 5 & 1 & 2 \\ 3 & 2 & 0 \\ 0 & 3 & 7 \end{bmatrix}$$

Now check $BB^{-1} = I$

$$\Rightarrow BB^{-1} = \begin{bmatrix} 2 & 5 & 4 \\ 1 & 1 & 2 \\ 3 & 3 & 5 \end{bmatrix} \begin{bmatrix} 5 & 1 & 2 \\ 3 & 2 & 0 \\ 0 & 3 & 7 \end{bmatrix} = \begin{bmatrix} 25 & 24 & 32 \\ 8 & 9 & 16 \\ 24 & 24 & 41 \end{bmatrix} \bmod 8$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$\Rightarrow$ B invertible since B^{-1} exist

* we note that $\frac{1}{2}$ and $\frac{1}{4}$ have no meaning since $2 \notin U(\mathbb{Z}_8)$ and $4 \notin U(\mathbb{Z}_8)$ $\Rightarrow \frac{1}{2}$ and $\frac{1}{4}$ are undefind in the Ring $\mathbb{Z}_8$

* Also we note that $\frac{1}{3}$, $\frac{1}{5}$ have meaning in $\mathbb{Z}_8$ since $3 \in U(\mathbb{Z}_8)$ and $5 \in U(\mathbb{Z}_8)$ so $3^{-1} \times 1 = 3 \in \mathbb{Z}_8$ and

$5^{-1} \times 5 = 5 \in \mathbb{Z}_8$

Question 3: If our ring is R, we know that $-4 = -1$ times 4. Let A be a ring with identity. Prove that $-a = -1 \cdot a$ for every $a \in A$

Solution:-

let $a \in A$ prove $-a = -1 \cdot a$ where $-a$ is the addative inverse

we know that $a \cdot 0 = 0 \cdot a = 0$

let $(1+(-1)) = 0$

So

$0 \cdot a = (1+(-1))a = (1+(-1)) = 0$

$\Rightarrow ((1+(-1))a = 1 \cdot a + (-1)a = 0$

$\Rightarrow 1 \cdot a + (-1)a = a + (-a) = 0$

$\Rightarrow 1 \cdot a = a$ and $(-1) \cdot a = -a$

There Fore $-a = (-1) \cdot a$.

2.2.10 Solution for HW-Seven

Farah Zeyad HW7
900086476

1) Let A be the ring Z_{12}. Find $Z(A)$, $Nil(A)$, $U(A)$ and $Id(A)$

Solution

$Z_{12} = \{1,2,3,4,5,6,7,8,9,10,11\}$

* $Z(A) \left\{ \begin{array}{l} 2\times6=0,\ 3\times4=0,\ 4\times9=0,\ 6\times6=0,\ 6\times10=0 \\ 8\times9=0,\ 8\times6=0 \end{array} \right\}$

$\Rightarrow Z(A) = \{0,2,3,4,6,8,9,10\}$

$Nil(A)$: let $a \in Z_{12}$ where $a^n = 0$ so we have $6^2 = 0$

$\Rightarrow Nil(A) = \{0,6\}$

$U(A) = U(Z_{12}) = U(12) = \{1,5,7,11\}$

$Id(A)$: let $a \in Z_{12}$ where $a^2 = a$ so we have $4^2 = 4$, $9^2 = 9$, $1^2 = 1$, 0

$\Rightarrow Id(A) = \{0,1,4,9\}$

2) let A be the ring $Z_n \oplus Z_m$. How many units (invertible element) does A have?

Solution :- Find $|U(A)|$

- we know (a,b) is invertible in A iff a is invertible in Z_n $(a \in U(Z_n) = U(n))$ and b is invertible in Z_m $(b \in U(Z_m) = U(m))$

- since $U(Z_n) = U(n)$ has $\phi(n)$ elements this mean a has $\phi(n)$ possiblity or choices

- since $U(Z_m) = U(m)$ has $\phi(m)$ elements this mean b has $\phi(m)$ possiblity or choices

There Fore (a,b) has $\phi(n)\phi(m)$ possiblity this mean $U(A)$ has $\phi(n)\phi(m)$ units. $\Rightarrow |U(A)| = \phi(n)\phi(m)$

$\Rightarrow$ There Fore A have $\phi(n)\phi(m)$ units

3) Let A be the ring $Z_6 \oplus Z_{14}$. Find Char(A). Find U(A).

Solution:-

- Find Char (A) where $A = Z_6 \oplus Z_{14}$
- $\text{Char}(\mathbb{Z}_6) = \text{char}((1)) = 6$

$\text{Char}(Z_{14}) = \text{char}((1)) = 14$

$\Rightarrow \text{char}(((1,1))) = \text{Lcm}(\text{char}(1), \text{char}(1))$

$= \text{Lcm}(6, 14) = \frac{6 \times 14}{\gcd(6,14)} = \frac{84}{2} = 42$

$= 42$

$\Rightarrow \text{Char}(A) = 42$

- Find $U(A) = U(Z_6 \oplus Z_{14}) = U(Z_6) \oplus U(\mathbb{Z}_{14})$
- $U(Z_6) = U(6) = \{1, 5\}$
- $U(14) = U(14) = \{1, 3, 5, 9, 11, 13\}$

$|U(\mathbb{Z}_6)| \oplus |U(Z_{14})|$

$= 2 \times 6 = 12$

$\Rightarrow$ Therefore $U(A) = \{(1,1), (1,3), (1,5), (1,9), (1,11), (1,13)\}$
$\{(5,1), (5,3), (5,5), (5,9), (5,11), (5,13)\}$

4) Let A be a ring such that $A = R_1 \oplus R_2$ where R_1 and R_2 are rings such that $|R_1| \geq 2$ and $|R_2| \geq 2$ Prove that A is never an integral Domain.

Let $a \in R_1$ and $b \in R_2$ Prove that A is not an integral domain

Since $a \in R_1$ then $(a,0) \in R_1 \oplus R_2$ and since $b \in R_2$ then $(0,b) \in R_1 \oplus R_2$.

$\Rightarrow (a,0) \odot (0,b) = (0,0)$

$\Rightarrow$ This mean $(a,0)$ and $(0,b)$ are Zero divisors

$\Rightarrow$ Since $(a,0)$ and $(0,b)$ are Zero divisors

$\Rightarrow$ Therefore A is not an integral domain

5) let A be a commutative ring with 1 $u \in U(A)$ and $w \in Nil(A)$

prove that $u+w \in U(A)$

Solution:

let $u \in U(A)$ and $w \in Nil(A)$ where $w^n = 0$, $n \geq 1$

prove $u+w \in U(A)$

$\Rightarrow$ $u+w = u(1+u^{-1}w)$, where $u^{-1}w \in Nil(A) \Rightarrow (u^{-1}w)^n = 0$

- if n is odd then we have

$(u^{-1}w)^n + 1 = (u^{-1}w+1)\left[(u^{-1}w)^{n-1} - (u^{-1}w)^{n-2} + \cdots + -(u^{-1}w) + \right]$

let $\left[(u^{-1}w)^{n-1} - (u^{-1}w)^{n-2} + \cdots + -(u^{-1}w) + 1\right] = a$

$\Rightarrow (u^{-1}w)^n + 1 = (u^{-1}w+1)\, a$ but $(u^{-1}w)^n = 0$ since $(u^{-1}w) \in Nil(A)$

$\Rightarrow$ $1 = (u^{-1}w+1)\, a$

$\Rightarrow$ There Fore $(u^{-1}w+1) \in U(A)$

$\Rightarrow$ $u+w = u(1+u^{-1}w)$, since $u \in U(A)$ and $(1+u^{-1}w) \in U(A)$

$\Rightarrow$ $u+w \in U(A)$

only Note if n is even we have $(u^{-1}w)^n = 0$ if i multiply it by $(u^{-1}w)$

we have $(u^{-1}w)(u^{-1}w)^n = (u^{-1}w) \cdot 0 \Rightarrow (u^{-1}w)^{n+1} = 0$ so $n+1$ is odd

so I can do the same step above:

$(u^{-1}w)^{n+1} + 1 = (u^{-1}w+1)\left[(u^{-1}w)^n - (u^{-1}w)^{n-1} + \cdots + -(u^{-1}w) + 1\right]$ so let

$\left[(u^{-1}w)^n - (u^{-1}w)^{n-1} + \cdots + -(u^{-1}w) + 1\right] = a$

$\Rightarrow$ since $(u^{-1}w)^{n+1} = 0$

$1 = (u^{-1}w+1)\, a \Rightarrow u^{-1}w+1 \in U(A)$

$\Rightarrow$ $u+w = u(u^{-1}w+1)$ since $u \in U(A)$ and $(u^{-1}w+1) \in U(A)$

$\Rightarrow$ $u+w \in U(A)$

6| let A be a Commutative ring with 1 and $e \in Id(A)$. prove that $1-e \in Id(A)$ and $1-2e \in U(A)$

Solution

- prove that $1-e \in Id(A)$, prove $(1-e)^2 = (1-e)$

$\Rightarrow (1-e)^2 = (1-e)(1-e) = 1+(-e)+(-e)+e^2$

$= 1+(-2e)+e^2$

since $e \in Id(A)$ $\Rightarrow e^2 = e$ $\Rightarrow = 1+(-2e)+e$

$= 1-e$

$\Rightarrow$ ThereFore $1-e \in Id(A)$

- prove that $1-2e \in U(A)$, Prove that $(1-2e)^2 = 1$

$\Rightarrow (1-2e)^2 = (1-2e)(1-2e) = 1+(-2e)+(-2e)+4e^2$

since $e \in Id(A)$

$e^2 = e \Rightarrow = 1+(-4e)+4e$

$= 1$

$\Rightarrow$ ThereFore $(1-2e) \in U(A)$.

7| let $B = \{0,3,6,9,12\}$ show that $(B,+,\cdot)$ is a subring of the ring $(\mathbb{Z}_{15},+,\cdot)$. IS B an ideal of $\mathbb{Z}_{15}$? Note that B is a ring too!. What is the "1" of the ring B? IS the "1" of B same "1" of $\mathbb{Z}_{15}$? what is the Char(B)? IS Char(B) defferent from Char($\mathbb{Z}_{15}$)? is B is a Feild?

Solution: By Constructing Caley's table For $(B,+)$ and $(B,\cdot)$

+	0	3	6	9	12
0	0	3	6	9	12
3	3	6	9	12	0
6	6	9	12	0	3
9	9	12	0	3	6
12	12	0	3	6	9

·	3	6	9	12
3	9	3	12	6
6	3	6	9	12
9	12	9	6	3
12	6	12	3	9

1) Show that $(B,+,\cdot)$ is a subring of the ring $(Z_{15},+,\cdot)$

- B is a subset of Z_{15}. $B \subseteq Z_{15}$
- $3+(-6) = 3+(9) = 12 \in B$, $3,6 \in B$
- $3 \times 6 = 18 \bmod 15 = 3 \in B$, $3,6 \in B$
- $0 \in B$ Addative inverse
- Addative inverse $-3 = 12$, $-6 = 9$

$\Rightarrow$ Therefore $(B,+,\cdot)$ is a subring of A.

2) Is B an ideal of Z_{15}?

yes, since b is a subring and also if we take For example $7 \in Z_{15}$ and $3 \in B$ this gives us $3 \times 7 = 21 \bmod 15 = 6$ where $6 \in B$

$\Rightarrow$ Therefore B is an ideal.

3) what is "1" of the ring B?

6 is the "1" multiplicative identity of B because $6 \times 3 = 3$, $6 \times 12 = 12$. , $6 \times 9 = 9$ Therefore "1" $= 6$

4) Is the "1" of the B the same "1" of Z_{15}?

No, because 6 is the multiplicative identity of B and 1 is the multiplicative identity of Z_{15}.

5) What is Char (B)?

The Char (B) is 5 because when we multiply The identity with 5 Gives zero where $5(6) = 6+6+6+6+6 = 0$ Therefore Char (B) = 5.

6) Is the Char (B) different from Char (Z_{15})? Yes because the Char (B) is 5 but Char (Z_{15}) = 15 because $1 \times 15 = 0$

IS B is a Feild? Yes

- B is a Commutative ring with identity "1" =6
  Since B is a Subring this mean it's a ring and each element is commutative like :-
  $3 \times 9 = 9 \times 3 = 12$, $3 \times 12 = 12 \times 3 = 6$
  So this mean B is an Abelian group under multiplication

- each Non-Zero element invertible under multiplication:
  $3 \times 12 = 6 \Rightarrow \bar{3}^{-1} = 12$, $9 \times 9 = 6 \Rightarrow \bar{9}^{-1} = 9$.

$\Rightarrow$ Since B is a Commutative ring with identity and each non-zero element in $U(B)$

$\Rightarrow$ Therefore B is a feild.

Also Note B has No zero divisor $Z(B) = \{0\}$ This mean B is a finite integral domain "From class Notes"
Every finite integral domain is a Feild

$\Rightarrow$ B is a Feild.

3 Section 3: Assessment Tools (unanswered)

3.1 Homework

3.1.1 HW-One

Name————————————, ID ——————

HW I (WARM UP), MTH 532, Spring 2020

Ayman Badawi

QUESTION 1. (i) Let D be a group and $a \in D$. Given $|a| = m < \infty$. Show that $D = \{a, a^2, a^3, ..., a^m\}$ is a subgroup of D with m elements [hint: Since D is finite, just show that D is closed]

(ii) Let D be a group and $a \in D$. Given $|a| = m < \infty$. Assume that $a^n = e$ (recall e is the identity of D). Prove that $m \mid n$.

(iii) Let D be a group and $a \in D$. Given $|a| = m < \infty$. Let $b \in D$ such that $b = a^k$ where $gcd(k, m) = 1$. Prove that $|b| = m$.

(iv) Let $D = (Z_{20}, +)$. Given $H = \{0, 4, 8, 12, 16\}$ is a subgroup of D. Find all left cosets of H.

(v) Let $D = (Q, +)$. Then $H = (Z, +)$ is a subgroup of $(Q, +)$. Prove that H has infinitely many left cosets. Give me 5 distinct left cosets of H.

(vi) Let $F = \{6, 12, 18, 24\}$. Convince me that F is a group under multiplication module 30 by constructing the Caley's Table. What is e? What is 12^{-1}? What is 24^{-1}?

Submit your solution on Saturday Feb 15, 2020 at 12.

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: `abadawi@aus.edu, www.ayman-badawi.com`

3.1.2 HW-Two

Name————————————, ID ——————

HW II , MTH 532, Spring 2020

Ayman Badawi

QUESTION 1. (i) Let D be a group, $a \in D$ such that $|a| = n < \infty$. Let m be a positive integer and $r = gcd(m, n)$. Prove that $|a^m| = n/r$. **I do not want to see a proof of this, the proof exists in the solution-book that I posted, but you need to know this fact and use it**

(ii) Let $D = (Z_{24}, +)$. Find $|9|$, $|14|$, $|18|$, $|11|$ (hint: note that $Z_{24} =< 1 >$ and for example $8 = 1^8$, then use (i)).

(iii) Let $a, b \in D$. Assume that $|b| = m < \infty$. Prove that $|a^{-1}ba| = m$.

(iv) Let $D = Z_n \oplus Z_m$, $n, m \geq 2$ (of course the binary operations are addition mod n and addition mod m). Let $(a, b) \in D$. Prove that $|(a, b)| = LCM[|a|, |b|]$ [hint: note that if k, w are integers, then LCM[k, w] = kw/gcd(k, w), for example LCM[8, 12] = 8.12/4 = 24]

(v) Let $D = Z_n \oplus Z_m$. Prove that D is cyclic if and only if $gcd(n, m) = 1$. [hint: use part IV]

(vi) Let $D = Z_6 \oplus Z_{14}$.

a. Convince me that D is not cyclic. Find the value of the integer m such that the order of each element in D is $\leq m$.

b. Find $|(3, 5)|$ and $|(4, 10)|$ [Hint: note $3 = 1^3$ and $5 = 1^5$, now use (i) and (iv)].

c. Give me two subgroups of D, say H_1, H_2 such that $|H_1| = |H_2| = 2$.

d. Does D have a cyclic subgroup of size (order) 21? If yes find a generator to such subgroup.

Submit your solution any time on SUNDAY before midnight, Feb 23, 2020 .

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: `abadawi@aus.edu, www.ayman-badawi.com`

3.1.3 HW-Three

HW III , MTH 532, Spring 2020

Ayman Badawi

QUESTION 1. (i) Fact (you may use it whenever it is needed, for a proof just see it in any Algebra TextBook, but you must KNOW this FACT). Let H be a subset of a group D (note that H can be finite or infinite). Then H is a subgroup of D if and only if $a^{-1} * b \in H$ for every $a, b \in H$ (a, b need not be distinct).

(ii) Let F, L be subgroups of a group D. Prove that $M = F \cap L$ is a subgroup of D (hint: Use (i) above)

(iii) by (ii), $N = 12Z \cap 15Z$ is a subgroup of $(Z, +)$. Since Z is cyclic, we know $N = aZ$. Find a.

(iv) Let D be an abelian group with 9 elements. Given that D has two distinct subgroups, H_1, H_2 such that $|H_1| = |H_2| = 3$. Convince me that it is impossible that $D = (Z_9, +)$. What will be an example of such group D?

(v) Let $f \in S_n$ such that f is m-cycle. Convince me that if m is odd integer, then $f \in A_n$ and if m is an even integer, then $f \notin A_n$.

(vi) Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 6 & 8 & 7 & 2 & 1 & 5 \end{pmatrix} \in S_8$.

a. Find $|f|$. Is $F \in A_8$? explain

b. Does A_8 has an abelian subgroup with 15 elements? [Hint: If you show that A_5 has a cyclic subgroup with 15 elements, then you are done, since cyclic implies abelian]

(vii) Let $f = (1\ 4\ 3)(1\ 4) \in S_4$. Find $|f|$. Let $k = (1\ 4\ 3)(1\ 5) \in S_5$. Find $|k|$.

(viii) Given $H = \{(1), (1\ 4\ 3), (1\ 3\ 4)\}$ is a subgroup of S_5 (this is given, you do not need to check unless you do not believe me). Find the left coset $(1\ 5)\ o\ H$ and find the right coset $H\ o(1\ 5)$. What do you observe? Can we say that H is a normal subgroup of S_5?

(ix) Let a, b be element of a group such that $a * b = b * a$. Assume $|a| = n$ and $|b| = m$. Let $k = |a * b|$. Prove $k \mid nm$.

(x) Give me an example of two elements a, b in a group where $|a| = n$, $|b| = m$ and $|a * b| = k$, but $k \nmid nm$ [hint: Stare at the element k in vii and some how find a and b !]

(xi) Let a, b be element of a group such that $a * b = b * a$. Assume $|a| = n$, $|b| = m$ and $gcd(n, m) = 1$. Let $k = |a * b|$. Prove $k = nm$.[Hint: you may want to use the fact from number theory that if $gcd(w, d) = 1$, $d \mid c$ and $w \mid c$, then $wd \mid c$, of course w, d, c are some positive integers]

(xii) Let $F : (D_1, *_1) \to (D_2, *_2)$ be a group-homomorphism and $H < D_1$. Prove that $F(H)$ is a subgroup of D_2 (note it is possible that $H = D_1$)[Hint: Use part (i) above]

(xiii) Let $F : (Z_{24}, +) \to (Z_{15}, +)$ be a group homomorphism such that $F(1) \neq 0$. Find $F(Z_{24})$. [Hint: Note that Z_n is cyclic, $F(Z_{24})$ is a subgroup of Z_{15} by xii and $|F(a)|$ must be a factor of $|a|$ for every $a \in Z_{24}$ by class-Theorem]. Find $F(1)$, $F(8)$, $F(12)$.

Submit your solution (by EMAIL) any time / all HWs must be submitted by Wed. before midnight, March 4, 2020 .

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: abadawi@aus.edu, www.ayman-badawi.com

3.1.4 HW-Four

Name————————————, ID ————————

HW IV , MTH 532, Spring 2020

Ayman Badawi

QUESTION 1. (i) Let D be a group with 27 elements. You just observed that $C(D)$ has at least 4 elements. Prove that D is abelian.

(ii) You need this fact, so you must know it and make use of it. Assume that H, K are subgroups of a group $(D,*)$. Note that $H*K = \{h*k \mid h \in H, k \in K\}$. Then $|H*K| = \frac{|H||K|}{|H\cap K|}$. (no proof is needed)

(iii) Let D be a finite group, K, H are normal subgroups of D such that $H*K = D$ and $H \cap K = \{e\}$.

a. Prove that $K \approx D/H$ [Hint note that $|D/H| = |K|$, define $f : K \to D/H$ such that $f(k) = k*H$ for every $k \in K$. Show that f is group homomorphism and then you only need to show that f is 1-1.]

b. Prove that $H \approx D/K$.

c. Prove that $D \approx \frac{D}{H} \oplus \frac{D}{K} \approx K \oplus H$. [hint: Define $f : D \to \frac{D}{H} \oplus \frac{D}{K}$ such that $f(d) = (d*H, d*K)$ for every $d \in D$. Show that f is a group homomorphism. Then show that f is 1-1 (note both groups have same cardinality. Then use (a) and (b) and finish the proof.)]

(iv) Let H, K be subgroups of a group D. In general, $H*K$ need not be a subgroup of D. However, if K is a normal subgroup of D, then prove that $K*H$ is a subgroup of D. [hint: Just show $a^{-1}*b \in K*H$ for every $a, b \in K*H$]

(v) Let D be a group with 38 elements, K, H are subgroups of D such that $|K| = 19$ and $|H| = 2$ such that H is a normal subgroup of D. Prove that $D \approx Z_{38}$ [hint: note that $|D/K| = 2$ and hence K is a normal subgroup of D by class notes and use (iii (c)), Show that D is cyclic and hence by class notes $D \approx Z_{38}$)]

(vi) Let D be an infinite cyclic group. Prove that D has exactly two generators. [Hint: We know $D \approx Z$. Hence how many generators does Z have?]

(vii) Let $U(n) = \{a \in Z_n | gcd(a,n) = 1\}$. Prove that $U(n)$ is a group under multiplication mod n with $\phi(n)$ elements. [Hint: Closure is clear, if $x, y \in U(n)$, then $gcd(x,n) = gcd(y,n) = 1$ and hence $gcd(xy,n) = 1$. Thus $xy \in U(n)$. To prove the inverse, you need to use Fermat-Euler result: let $a \in U(n)$, since $gcd(a,n)$ we know that $n|(a^{\phi(n)} - 1)$ and this means that $a^{\phi(n)} = 1$ mod(n). Thus $a^{-1} = a^{(\phi(n)-1)}\ mod(n)$]. Example: $U(12) = \{1, 5, 7, 11\}$ is a group (abelian) with $\phi(12) = 4$ elements under multiplication mod(12).

(viii) (must KNOW, no need for a proof, nice result on $U(n)$) . Assume $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ (prime factorization of n where $p_1 < p_2 < \cdots < p_k$). Then we know $\phi(n) = (p_1-1)p_1^{(\alpha_1-1)}\cdots(p_k-1)p_k^{(\alpha_k-1)}$. Then (BEAUTIFUL RESULT) If n is even then $(p_1 = 2)$ and

$U(n) \approx Z_2 \oplus Z_{2^{(\alpha_1-2)}} \oplus Z_{(p_2-1)} \oplus Z_{p_2^{(\alpha_2-1)}} \oplus \cdots \oplus Z_{(p_k-1)} \oplus Z_{p_k^{(\alpha_k-1)}}$. (note if $\alpha_1 = 1$ then remove $Z_2 \oplus Z_{2^{(\alpha_1-2)}}$, note $U(2) = \{1\}$). If n is odd, then

$U(n) \approx Z_{(p_1-1)} \oplus Z_{p_1^{(\alpha_1-1)}} \oplus Z_{(p_2-1)} \oplus Z_{p_2^{(\alpha_2-1)}} \oplus \cdots \oplus Z_{(p_k-1)} \oplus Z_{p_k^{(\alpha_k-1)}}$. Example Assume $n = 2^3 5^7 11^3$. Hence $\phi(n) = 2^2(4)5^6(10)11^2$. (n is even). Hence $U(n) \approx Z_2 \oplus Z_2 \oplus Z_4 \oplus Z_{5^6} \oplus Z_{10} \oplus Z_{11^2}$. Example $n = (2)7^8 13^2$. (n is even). $\phi(n) = (6)7^7(12)13^1$. Hence $U(n) \approx Z_6 \oplus Z_{7^7} \oplus Z_{12} \oplus Z_{13}$

(ix) Prove that $U(n)$, $n \geq 3$, is cyclic if and only if $n = 4$ or $n = p^k$ or $n = 2p^k$ for some ODD prime p and $k \geq 1$. [hint: note that if p is prime odd then $gcd(p-1, p) = 1$, also note that if p is odd, then p -1 is even. Use (viii) and old HW!).

(x) Prove that $U(64)$ has an element of order 16, but it has no elements of order 32. (Hint: of course you are not going to calculate the order of each element!, use (viii) and old HW).

(xi) Prove that $D = (Z_5, +) \oplus U(18)$ is cyclic, and hence $D \approx (Z_m, +)$. Find m.

(xii) prove that $(Q^*, .)$ is not cyclic. [Hint: We know Q^* is a group under normal multiplication. Note that in an infinite cyclic group D we have $|a| = \infty$ for each $a \in D - \{e\}$ (class notes).

Submit your solution (by EMAIL) any time / all HWs must be submitted by Wed. before midnight, March 18, 2020 .

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: `abadawi@aus.edu`, `www.ayman-badawi.com`

3.1.5 HW-Five

Name————————————, ID ——————

HW V , MTH 532, Spring 2020

Ayman Badawi

Observations

(i) Let p, q be two primes numbers (p, q need not be distinct) If H, K are two distinct groups with p elements and q elements, respectively, then $H \cap K = \{e\}$. Note that if p = q, but H, K are distinct, we still have $H \cap K = \{e\}$.

(ii) If $|H| = p^m and |K| = q^n$, where q, p are distinct prime integers, then $H \cap K = \{e\}$.

(iii) If $D = Z_5 \oplus Z_{25} \oplus Z_3$, then D has many subgroups with 25 elements. For, let H be a subgroup of Z_{25} with 5 elements. We know that such H is unique (since Z_{25} is cyclic). Hence $W = Z_5 \oplus H \oplus \{0\}$ and $K = \{0\} \oplus Z_{25} \oplus \{0\}$ are subgroups with 25 elements. Also since $|(a, 1, 0)| = 25$ for every $a \in Z_5$, we conclude that for each $a \in Z_5$, the group F_a generated by (a, 1, 0) is a cyclic subgroup of D with 25 elements. Also note that W, K, F_a $(a \neq 0)$ are distinct subgroups and each is with 25 elements, note if a = 0, then $F_a = K$.

QUESTION 1. Let D be an abelian group with $2^3 5^2$ elements

(i) Suppose that D has exactly one subgroup with 4 elements. Find all non-isomorphic groups with these properties. [hint: Observations above might be useful]

(ii) Suppose that D has exactly one subgroup with 4 elements and it has exactly one subgroup with 5 elements. Find all non-isomorphic groups with these properties.

QUESTION 2. Let D be a cyclic group with 100 elements. Convince me that $(AUT(D), o)$ is an abelian group and find $m_1, ..., m_k$ such that $AUT(D) \approx Z_{m_1} \oplus \cdots \oplus Z_{m_k}$. [hint: Use my lecture! and HW 4].

QUESTION 3. Prove that every group with $n = 17.3^2$ is abelian. Find all non-isomprphic groups with n elements. [Hint: See my first lecture on Sylow !]

QUESTION 4. Let D be a group with 5.11.29. Prove that D has exactly one subgroup with 29 elements, say H, and $H \subseteq C(D)$. [hint: see my part 2 lecture on sylows].

QUESTION 5. Let D be a group with 216 elements. Prove that D is not simple. [hint: note that $216 = 2^3.3^3$ and it is possible that $n_3 = 4$. Use the technique as in my part 2 lecture on Sylow's Theorem to construct a group homomorphism with non-trivial kernel.]

QUESTION 6. Let D be a group with 5.7.17 elements. Prove that D is not simple. Assume that $n_{17} \neq 1$. How many elements in D have order 17? [hint: Find n_5...so you may discover that D is not simple. see OBSERVATION (i) above..., then it should be clear how many elements in D have order 17]

Submit your solution (by EMAIL) any time by Wed. before midnight, March 25, 2020 .

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: `abadawi@aus.edu, www.ayman-badawi.com`

3.1.6 HW-Six

HW six , MTH 532, Spring 2020

Ayman Badawi

(1) you need to know this fact: Fix $n \geq 2$ and A be a commutative ring with 1. Then $B \in U(A^{n\times n})$ if and only if $|A| \in U(A)$, i.e. using street language , an $n \times n$ matrix B is invertible over A if and only if determinant of B is a unit of A (an element in a ring A is called unit, if it has inverse under multiplication)

For example A matrix $B \in U(Z_m^{n\times n})$ if and only if $|B| \in U(Z_m) = U(m)$. A matrix $B \in U(Z^{n\times n})$ if and only if $|B| \in U(Z) = \{1, -1\}$

(2) You need to know the meaning of FRACTIONS in a ring: Let A be a commutative ring with 1 and $a, b \in A$. Then $\frac{a}{b}$ has a meaning in A if and only if $b \in U(A)$. If $b \in U(A)$, then $\frac{a}{b}$ means $b^{-1}a$.

For example $\frac{4}{5}$ has a meaning in the ring Z_6 since $5 \in U(Z_6) = U(6)$ and $\frac{4}{5}$ means the element $5^{-1}4 = 2 \in Z_6$. Since $4 \notin U(Z_{14}) = U(14)$, $\frac{5}{4}$ is undefined in the ring Z_{14}.

QUESTION 1. Let $F = \{1, 2, 3, 4\}$ and $A = P(F)$ ($P(F)$ is the power set of F, note $|P(F)| = 16$). We know (A, +, .) is a commutative ring with identity $1 = F$ (see class notes, $a + b = (a - b) \cup (b - a)$ and $ab = a \cap b$ for every $a, b \in A$). Also, we know that $U(A) = \{F\}$ and hence a matrix $B \in U(A^{n\times n})$ if and only if $|B| = F$. Also, from class notes, we know $-a = a$ and $a^2 = a$ for every $a \in A$

For example $B = \begin{bmatrix} \{1,3\} & \{2,4\} \\ \{1,2,4\} & \{1,2,3\} \end{bmatrix} \in U(F^{2\times 2})$. You only need to know what + means and what . means in the ring A. Then all techniques you learned from basic linear algebra can be applied on A. In a basic linear algebra course your ring is R, but here your ring is A.

For example we know that if $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is invertible over R then $B^{-1} = \frac{1}{|B|}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. We can use this fact for any 2×2 matrix over a commutative ring with identity.

So $|B| = \{1,3\}\{1,2,3\} + -\{2,4\}\{1,2,4\} = \{1,3\} \cap \{1,2,3\} + \{2,4\} \cap \{1,2,4\} = \{1,3\} + \{2,4\} = (\{1,3\} - \{2,4\}) \cup (\{2,4\} - \{1,3\}) = \{1,2,3,4\} = F \in U(A)$. Hence B is invertible. Thus $B^{-1} = \frac{F}{F}\begin{bmatrix} \{1,2,3\} & \{2,4\} \\ \{1,2,4\} & \{1,3\} \end{bmatrix} = F\begin{bmatrix} \{1,2,3\} & \{2,4\} \\ \{1,2,4\} & \{1,3\} \end{bmatrix} = \begin{bmatrix} \{1,2,3\} & \{2,4\} \\ \{1,2,4\} & \{1,3\} \end{bmatrix}$

Note that $BB^{-1} = B^{-1}B = \begin{bmatrix} F & \phi \\ \phi & F \end{bmatrix} = I_2$ since in our A, $1 = F$ and $0 = \phi$.

(i) Let $B = \begin{bmatrix} \{1,2\} & \{2,4\} \\ \{3,4\} & \{1,3\} \end{bmatrix}$. Does B^{-1} exist? if yes, then find it. If no, then explain.

(ii) Let $B = \begin{bmatrix} \{2,3\} & \{1,3,4\} \\ \{1,3,4\} & \{2,4\} \end{bmatrix}$. Does B^{-1} exist? if yes, then find it. If no, then explain.

(iii) Let $B = \begin{bmatrix} F & \{2,4\} & \{1\} \\ \{1,3\} & F & \{3\} \\ \{2\} & \{2\} & F \end{bmatrix}$. If possible find B^{-1} [Hint: Use the techniques you learned from linear Algebra.

Use row operations and try to change the matrix $[B| \begin{bmatrix} F & \phi & \phi \\ \phi & F & \phi \\ \phi & \phi & F \end{bmatrix}$ into $[\begin{bmatrix} F & \phi & \phi \\ \phi & F & \phi \\ \phi & \phi & F \end{bmatrix} |C]$. If you succeed then $C = B^{-1}$, if you did not succeed, then B is not invertible over A.

QUESTION 2. Convince me that $B = \begin{bmatrix} 2 & 5 & 4 \\ 1 & 1 & 2 \\ 3 & 3 & 5 \end{bmatrix}$ is invertible over Z_8. Again use the techniques you learned in linear algebra but here addition means addition mod 8 and multiplication means multiplication mod 8 and in view of the comments in (2) observe that $1/2, 1/4$ have no meaning in Z_8 but $1/3, 1/5$ have meaning!.

QUESTION 3. If our ring is R, we know that -4 = -1 times 4. Let A be a ring with identity. Prove that $-a = -1.a$ for every $a \in A$ (i.e., prove that the additive inverse of a equals the additive inverse of the identity "1" times a). (Hint: use that fact that $a.0 = 0 = 0.a = 0$ for every $a \in A$)

Submit your solution (by EMAIL) any time by Friday midnight, April 17, 2020 .

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: abadawi@aus.edu, www.ayman-badawi.com

3.1.7 HW-Seven

Name————————————, ID ——————

HW SEVEN , MTH 532, Spring 2020

Ayman Badawi

QUESTION 1. Let A be the ring Z_{12}. Find $Z(A)$, $Nil(A)$, $U(A)$ and $Id(A)$.

QUESTION 2. Let A be the ring $Z_n \oplus Z_m$. How many units (invertible elements) does A have? i.e., Find $|U(A)|$ [Hint: it is trivial to see that (a, b) is invertible in A iff a is invertible in Z_n and b is invertible in Z_m, some how the question is related to $\phi(k)$]

QUESTION 3. Let A be the ring $Z_6 \oplus Z_{14}$. Find $Char(A)$. Find $U(A)$.

QUESTION 4. Let A be a ring such that $A = R_1 \oplus R_2$, where R_1 and R_2 are rings such that $|R_1| \geq 2$ and $|R_2| \geq 2$. Prove that A is never an integral domain.

QUESTION 5. Let A be a commutative ring with 1, $u \in U(A)$ and $w \in Nil(A)$. Prove that $u + w \in U(A)$. (hint: Note that $u + w = u(1 + u^{-1}w)$ and $u^{-1}w \in Nil(A)$. Also note that if m is an odd integer, then high school math tells us that $x^m + 1 = (x + 1)[(x^{m-1} - x^{m-2} + ... + -x + 1])$

QUESTION 6. Let A be a commutative ring with 1 and $e \in Id(A)$. Prove that $1 - e \in Id(A)$ and $1 - 2e \in U(A)$.

QUESTION 7. Let $B = \{0, 3, 6, 9, 12\}$. Show that $(B, +, .)$ is a subring of the ring $(Z_{15}, +, .)$. Is B an ideal of Z_{15}? note that B is a ring too!. What is "1" of the ring B? Is the "1" of B the same "1" of Z_{15}? What is $Char(B)$? Is Char(B) different from $Char(Z_{15})$? Is B a field? [hint: Just do the Caley's table of (B, +) and the Caley's table of (B, .), stare really well, then start answering the questions!, remember + means addition mod 15 and . means multiplication mod 15]

Submit your solution (by EMAIL) any time by Monday midnight, April 27, 2020 .

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: `abadawi@aus.edu, www.ayman-badawi.com`

3.2 Exams

3.2.1 Exam One

Name——————————————, ID ———————

EXAM I , MTH 532, Spring 2020

Ayman Badawi

QUESTION 1. Given D is a group with 48 elements. Assume that D has an element $a \in C(D)$ such that $|a| = 16$. Prove that D is cyclic.

QUESTION 2. Does $U(54)$ have an element of order 18? If yes, how many elements of order 18 does U(54) have?

QUESTION 3. Let $f : (Z_{18}, +) \to (U(50), .)$ be a group homomorphism such that $f(1) \neq 1$. Find $f(0)$. Find $Ker(f)$.

QUESTION 4. Let D be a group with 100 elements. Assume that D has a subgroup H with 20 elements such that $H \subseteq C(D)$. Prove that D is an abelian group.

QUESTION 5. (i) **EXTRA CREDIT, but you need it to solve (ii)**. Let D be a finite group and H be a subgroup of D such that $[D : H] = m$ for some integer m (note that $[D : H] = |D|/|H|$ = number of all distinct left cosets of H). Prove that there is a group homomorphism , say f, from D into S_m such $Ker(f) \subseteq H$.

(ii) Let D be a finite simple group. Assume that H, K are subgroups of D such that $[D : H] = p_1$ and $[D : K] = p_2$ for some prime integers p_1, p_2. Prove that $p_1 = p_2$. (nice result!)

QUESTION 6. Let D be a group with p^m elements, where p is a prime integer and $m \geq 2$. Prove that D has a normal subgroup with p^{m-1} elements. [Hint : Show that D must have a subgroup H with p^{m-1} elements by class note result (which result?). Then use class - lecture (result) to show that H is normal in H (which result?)].

QUESTION 7. Let D be a group with $(5^2)(7^2)$ elements. Prove that D is an abelian group. Find all non-isomorphic groups with $(5^2)(7^2)$ elements?

QUESTION 8. Let $a = (1\ 2\ 3)\ o\ (1\ 3\ 4\ 2\ 5) \in S_6$. Is $a \in A_6$? Find $|a|$.

QUESTION 9. Let D be a group with 105 elements (105 = (3)(5)(7)).

(i) Prove that D is not simple. [Hint: Assume D is simple. How many elements of orders 7, 5, 3 does D have? is this possible?

(ii) Assume that $n_7 = 1$ (i.e., D has exactly one sylow-7-subgroup). Prove that D has a normal cyclic subgroup with 35 elements [hint: Use a result from HW, use a result from class notes! and of course sylow's theorems] .

Submit your solution by 3 pm (as at most), March 28, 2020 .

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: `abadawi@aus.edu`, `www.ayman-badawi.com`

3.2.2 Exam Two

Name——————————————, ID ——————

EXAM II , MTH 532, Spring 2020

Ayman Badawi

Submit your solution any time before 00: 15, (I will deduct points after 00 : 17) .

QUESTION 1. (i) Let A be a commutative ring with 1 and B be a commutative ring (B may not have "1"). Assume $f : A \to B$ is a ring-homomorphism. Prove that $f(1) \in Id(B)$ (i.e., show that $f(1)$ is an idempotent element of B).

(ii) Let A be a commutative ring with 1 and $B = 2Z$ (B is the set of all even integers). Assume $f : A \to B$ is a ring-homomorphism. Prove that $f(a) = 0$ for every $a \in A$.

(iii) Let A, B be fields and $f : A \to B$ is a ring-homomorphism such that $f(a) \neq 0$ for some $a \in A$. Prove that f is injective (i.e., prove that f is one-to-one).

(iv) Let $f : Z_6 \to Z_9$ be a ring-homomorphism. Prove that $f(a) = 0$ for every $a \in Z_6$.

QUESTION 2. Let A be a commutative ring with 1 and let I be a proper ideal of A that is not a maximal ideal of A. Hence, we know that $I \subset M$ for some maximal ideal M of A. Let $a \in M - I$. Prove that $a + I$ is not an invertible element of the ring A/I (i.e., show that $a + I \notin U(A/I)$).

QUESTION 3. Let A be a finite commutative ring with 1 and $a \in A$. Suppose that $a \notin Z(A)$. Prove that $a \in U(A)$.

QUESTION 4. Let A be a commutative ring with 1 and $f(X) \in A[X]$ such that $f(X) \neq 0$ and $f(X) \in Z(A[X])$. For every $n \geq 1$, prove that there exists a polynomial $k(X) \in A[X]$ of degree n such that $k(X)f(X) = 0$.

QUESTION 5. Let A be a commutative ring with 1 and I be a prime ideal of A. Prove that $Nil(A) \subseteq I$.

QUESTION 6. (i) Let $A = Z_4 \oplus Z_6$. Find all prime ideals of A.

(ii) Let $A = Z_{12} \oplus Z_8$. Find $Nil(A)$.

(iii) Let $B = \begin{bmatrix} 2 & 4 \\ 2 & 2 \end{bmatrix}$. Is B invertible over Z_9? If yes, then find B^{-1}. If No, then explain.

(iv) Let $A = Z_{10}[X]$ and $f(X) = 2X^3 + 5X + 4 \in A$. Is $f(X) \in Z(A)$?

(v) Give me an example of a commutative ring A with 1 such that $Char(A) = 5$ and $Z(A) \neq \{0\}$.

(vi) Let $A = Z_{18}[X]$ and $f(X) = 6X^2 + 12X + 17 \in A$. Is there a polynomial $k(X) \in A$ such that $k(X)f(X) = 1$? If yes, then explain (you do not need to find k(X)). If no, then tell me why not.

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: `abadawi@aus.edu, www.ayman-badawi.com`

3.2.3 Final Exam

Final Exam , MTH 532, Spring 2020

Ayman Badawi

QUESTION 1. Let F be a finite field with 2^{12} elements.

(i) **(3 points)** Let $a \in F$. Then a is a root of an irreducible monic polynomial of degree m over Z_2 Find all possibilities of m.

(ii) **(3 points)** We know that $(F^*, .)$ is a cyclic group and hence $(F^*, .) =< a >$ for some $a \in F^*$. Prove that the degree of $Irr(a, Z_2) = 12$? (i.e., prove that the degree of the unique irreducible monic plolynomial over Z_2 that has a as a root is 12)

(iii) **(3 points)** We know $|F^*| = 2^{12} - 1 = 4095$. Since $819 \mid 4095$, then we know that F^* has a unique cyclic subgroup, say $H =< b >$ for some $b \in F^*$ with 819 elements. What is the degree of $Irr(b, Z_2)$? **justify your answer**

(iv) **(4 points)** Let P_{12} be the set of all irreducible monic polynomials of degree 12 over Z_2. Find $|P_{12}|$. Show the work.

(v) **(8 points)** Find all elements of the Galois group $Aut(F/Z_2)$. For each subgroup H of $Aut(F/Z_2)$ find the corresponding subfield of F, say L_H, that is fixed by H.

QUESTION 2. Let E be the 5th cyclotomic extension field of Q

(i) **(2 points)** $E = Q(a)$ for some $a \in C$ (C is the ring (field) of all complex numbers). Find a.

(ii) **(6 points)**Let a as in (i), find $Irr(a, Q)$, find $[E : Q]$, and find all roots of $Irr(a, Q)$ inside E. Is $Aut(E/Q)$ a cyclic group under composition? how many elements does $Aut(E/Q)$ have?

(iii) **(2 points)** Find a basis B (in terms of a) of E over Q.

(iv) **(2 points)** write $a^6 + a^5 + a^4$ as a linear combination of the elements in the basis B (B is as in iii).

(v) **(4 points)** For each subgroup of $Aut(E/Q)$ with 2 elements, say H, find the corresponding subfield of E, say L_H, that is fixed by H.

QUESTION 3. Let $E = Q(\sqrt{5}, \sqrt{7})$.

(i) **(3 points)**. We know that $E = Q(a)$ for some $a \in R$. Find $Irr(a, Q)$ (i.e., find the unique irreducible monic polynomial over Q that has a as a root. What is $[E : Q]$?

(ii) **(3 points)** It is clear that $L = Q(\sqrt{35})$ is a subfield of E. Find the subgroup, say H, of $Aut(E/Q)$ that fixes the field L.

(iii) **(3 points)** Is the field $Q(\sqrt{5})$ isomorphic to the field $Q(\sqrt{7})$? If yes, then construct such ring-isomorphism (field-isomorphism)? If no, then explain briefly why not?

QUESTION 4. (3 points) Let E be the splitting field of the polynomial $f(x) = x^7 - 18$. We know that E is a Galois Extension of Q. Prove that $Aut(E/Q)$ is a non-abelian group.

QUESTION 5. (i) **(2 points)** Give me an example of an integral domain that is not a UFD (Unique Factorization Domain).

(ii) **(2 points)** Give me an example of a Unique Factorization Domain that is not a principal ideal domain

(iii) **(4 points)** Let A be a principal ideal domain. Prove that every prime ideal of A is a maximal ideal of A.[Hint: Every proper ideal is a principal ideal, and every proper ideal is contained in a maximal ideal].

(iv) **(4 points)** Let A be a commutative ring with 1. Suppose that A has exactly one maximal ideal. Prove that $Id(A) = \{0, 1\}$. [Hint: note if $x \notin U(A)$, then the ideal $(x) = xA$ is a proper ideal of A].

(v) **(4 points)** Let A be an integral domain, P be a prime ideal of A, and I be a proper ideal of A such that $I \cap P = \{0\}$. Prove that there exists a prime ideal F of A such that $I \subseteq F$ and $F \cap P = \{0\}$ [Hint: Let $W = P - 0$, note $I \cap W = \emptyset$]

QUESTION 6. (4 points). Let F be a group with 12 elements. Prove that F must have a normal subgroup with 3 elements **OR** F must have a normal subgroup with 4 elements.

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: `abadawi@aus.edu, www.ayman-badawi.com`

Faculty information

Ayman Badawi, American University of Sharjah, UAE.
E-mail: abadawi@aus.edu