Department of Mathematics, METU, MATH 116 - BASIC ALGEBRAIC STRUCTURES

FINAL EXAMINATION

10th June 2016. Duration : 150 minutes. 6 6 8

Five questions : $6 + (4 + 3) + (4 + 3)$, $10 + 5 + 5$, $10 + 7 + 3$, $8 + 7 + 5$, $\cancel{5} + \cancel{7} + \cancel{6}$

STUDENT NUMBER	NAME, FAMILY NAME

Q1	Q2	Q3	Q4	Q5	TOTAL

Solutions

1. (A) Decompose

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 6 & 7 & 5 & 2 & 4 & 8 & 1 & 11 & 9 & 10 \end{bmatrix} \in S_{11}$$

into a product of disjoint cycles.

(B) Compute the parity and the order of σ .

(C) Let U_n be the group of invertible elements of $\mathbb{Z}_n$ with respect to multiplication modulo n. Prove that U_{14} is cyclic and find a subgroup of S_{11} that is isomorphic to U_{14} .

(A) $\sigma = \underbrace{(1\ 3\ 7\ 8)}_{\sigma_1}\underbrace{(2\ 6\ 4\ 5)}_{\sigma_2}\underbrace{(9\ 11\ 10)}_{\sigma_3}$

(B) σ_1 & σ_2 are odd, σ_3 is even, hence $\sigma = \sigma_1\sigma_2\sigma_3$ is even

$\text{Order}(\sigma) = \text{LCM}\big(\underbrace{\text{order}(\sigma_1)}_{=4}, \underbrace{\text{order}(\sigma_1)}_{=4}, \underbrace{\text{order}(\sigma_2)}_{=3}\big) = 12$

least common multiple

(C) $U_n = \{[1], [3], [5], [9], [11], [13]\}$ is a cyclic group.

Indeed U_n is generated by $[3]$.

Thus, if $\tau \in S_{11}$ is an arbitrary cycle of length 6, (such as $\tau = (1\ 2\ 3\ 4\ 5\ 6)$) $\langle \tau \rangle \cong U_{11}$ as cyclic groups of the same order are isomorphic.

2. Let G be a group, H be a subgroup of G, N be a normal subgroup of G.

(A) Prove that $HN = \left\{xy \;\middle|\; x \in H, y \in N\right\}$ is a subgroup of G. (Hint : Remember that $aN = Na$ or equivalently $aNa^{-1} = N$ for any $a \in G$ and $xyx'y' = xx'(x')^{-1}yx'y'$ for any $x, x' \in H, y, y' \in N$.)

(B) Prove that $H \cap N$ is a normal subgroup of H.

(C) Suppose that G/N is abelian. Show that $xyx^{-1}y^{-1} \in N$ for all $x, y \in G$.

(A) Given $g, g' \in HN$, there exist $x, x' \in H$ & $y, y' \in N$ such that $g = xy$, $g' = x'y'$ hence

$$gg' = xyx'y' = xx'\left((x')^{-1}y\,x'\right)y' \in H$$

as $x, x' \in H$ & $(x')^{-1}y\,x', y' \in N$.

Similarly

$$g^{-1} = y^{-1}x^{-1} = x^{-1}(x y^{-1} x^{-1}) \in HN$$

as $x \in H$ and $x^{-1}y^{-1}x \in N$.

(B) For arbitrary $x \in H$ & $a \in H \cap N$, clearly $xax^{-1} \in H$ and $xax^{-1} \in N$. Consequently $x(H\cap N)x^{-1} \subseteq H \cap N$. This being true for arbitrary $x \in H$, it follows that $H \cap N$ is normal in H.

(C) Since G/N is abelian, for any $x, y \in G$

$xyx^{-1}y^{-1}N = (xN)(yN)(x^{-1}N)(y^{-1}N) = eN = N$, hence $xyx^{-1}y^{-1} \in N$.

3. Given a nonempty set U, let $\mathfrak{P}(U)$ be the set of all subsets of U. Consider the binary operations $\oplus$ and $\odot$ on $\mathfrak{P}(U)$ defined for each $X, Y \in \mathfrak{P}(U)$ by

$$X \oplus Y = (X \cup Y) - (X \cap Y) \quad \text{and} \quad X \odot Y = X \cap Y.$$

(Both these operations may be assumed to be commutative and associative and $\odot$ may be assumed to be distributive over $\oplus$ <u>without proof.</u>)

(A) Prove that $\mathfrak{P}(U)$ constitutes a commutative ring with $1 \neq 0$ with respect to the binary operations $\oplus$ and $\odot$.

(B) Let $U = \{a, b\}$. Find the set of zero divisors in $\mathfrak{P}(U)$.

(C) Is $\mathfrak{P}(U)$ with respect to $\oplus$ and $\odot$ an integral domain ?

(A) It is sufficient to notice the following :

- $\emptyset \in \mathcal{P}(U)$ is the additive identity, the "0" in $\mathcal{P}(U)$ as
$$A \oplus \emptyset = (A \cup \emptyset) - (A \cap \emptyset) = A - \emptyset = A \quad \text{for any } A \in \mathcal{P}(U)$$
- $A \in \mathcal{P}(U)$ is the additive inverse, the "$-A$" of A in $\mathcal{P}(U)$ as
$$A \oplus A = (A \cup A) - (A \cap A) = A - A = \emptyset$$
- $\mathcal{P}(A)$ is obviously closed under $\oplus$
- $\mathcal{P}(A)$ is closed under $\odot$
- $U \in \mathcal{P}(U)$ is the multiplicative identity, the "1" in $\mathcal{P}(U)$ (Clearly $1 \neq 0$) as
$$A \odot U = A \cap U = A.$$

(B) $\mathcal{P}(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \underset{=\{a,b\}}{U}\}$. The elements $\{a\}, \{b\} \in \mathcal{P}(\underset{=\{a,b\}}{U})$ are zero divisors as
$$\{a\} \odot \{b\} = \{a\} \cap \{b\} = \emptyset, \ \& \ \{a\} \neq \emptyset \ \& \ \{b\} \neq \emptyset.$$

The sole remaining <u>non zero element</u> $U \in \mathcal{P}(U)$ is <u>not</u> a zero divisor as $U \odot U = U \neq \emptyset$, $U \odot \{a\} = \{a\} \neq \emptyset$, $U \odot \{b\} = \{b\} \neq \emptyset$

(C) As $\mathcal{P}(U)$ contains zero divisors, it is <u>not</u> an integral domain.

4. Let R be commutative ring with $1 \neq 0$ and let I be an ideal in R.

(A) If there exists $x \in I - \{0\}$ which has a multiplicative inverse, (that is , x is a "unit") prove that $I = R$.

(B) For any $a \in R$, prove that

$$J = aR = \left\{ ax \;\middle|\; x \in R \right\}$$

is an ideal in R.

(C) If a commutative ring S with $1 \neq 0$ has no nontrivial ideal, prove that S is a field.

(A) Suppose that $xy = 1$. Thus, for any $r \in R$ r

$$r = ryx = \underbrace{(ry)}_{\in R}\underbrace{x}_{\in I} \in I.$$

Hence $R \subseteq I$.

(B) If $b, b' \in J$, $\exists$ $x, x' \in R$ with $b = ax$, $b' = ax'$ hence

$$b + b' = ax + ax' = a\underbrace{(x+x')}_{\in R} \in J.$$

$$-b = a\underbrace{(-x)}_{\in R} \in J$$

and for arbitrary $b \in J$ and $r \in R$, $\exists$ $x \in R$ with $b = ax$ and

$$rb = rax = a\underbrace{rx}_{\in R} \in J.$$

$0 \in J \neq \emptyset$. Hence J is an ideal in R.

(C) For each $x \in S - \{0\}$, xS is an ideal in S and $xS \neq \{0\}$ as $x = x \cdot 1 \in xS$. Hence $xS = S$. Therefore $\exists y \in S$ such that $xy = 1 \in S$. This being true for arbitrary $x \in S$,

S is a field.

5. Decide if the following polynomials are irreducible in the indicated polynomial rings. If not irreducible, find the irreducible factors, show that they are indeed irreducible:

(A) $x^3 + x + 1 \in \mathbb{Z}_2[x]$.
(B) $x^3 + x + 1 \in \mathbb{Z}_3[x]$.
(C) $x^6 + 1 \in \mathbb{R}[x]$.

(A) $p(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ has no roots in $\mathbb{Z}_2$ as $p(0) = 1$, $p(1) = 1$

therefore it is irreducible.

(B) $q(x) = x^3 + x + 1 \in \mathbb{Z}_3[x]$ is ~~redu~~ divisible by $x - 1$ as $q(1) = 0$.

Indeed

$$x^3 + x + 1 = (x-1)(x^2 + x - 1)$$

where $x^2 + x - 1 \in \mathbb{Z}_3[x]$ is irreducible as it has no roots in $\mathbb{Z}_3$

(C)

$$x^6 + 1 = (x^2+1)(x^4 - x^2 + 1)$$
$$= (x^2+1)\left[(x^2+1)^2 - 3x^2\right]$$
$$= (x^2+1)(x^2 + \sqrt{3}\,x + 1)(x^2 - \sqrt{3}\,x + 1)$$

all of theses three factors are irreducible since they ~~h~~ have no roots in $\mathbb{R}$

$$x^2 \mp \sqrt{3}\,x + 1 = \left(x \mp \frac{\sqrt{3}}{2}\right)^2 + \frac{1}{4} > 0$$