Department of Mathematics

University of Pittsburgh

MATH 0430 (Abstract algebra)

Midterm 2, Fall 2011

Instructor: Kiumars Kaveh

Last Name: **Student Number:**

First Name:

TIME ALLOWED: 1 HOUR AND 20 MINUTES. TOTAL MARKS: 100
NO AIDS ALLOWED. WRITE SOLUTIONS ON THE SPACE PROVIDED.

Question	Mark
1	/10
2	/10
3	/20
4	/15
5	/10
6	/10
7	/10
8	/15
9	/2
TOTAL	/100 + 2

1(a).[5 points] State Fundamental Homomorphism Theorem.

Let $\phi : G \longrightarrow G'$ be a homomorphism between groups G and G'. Let $\phi[G]$ denote the image of ϕ (it is a subgroup of G'). Then

$$G/\ker(\phi) \cong \phi[G].$$

(b).[5 points] Give definition of *one* of the following: (1) integral domain, or (2) action of a group G on a set X.

1) An integral domain is a ring R such that:

a) R has 1 (i.e. identity for multiplication).

b) R is commutative.

c) R has no zero divisors (i.e. if $ab = 0$ for $a, b \in R$ then $a = 0$ or $b = 0$).

2) An action of G on a set X is a map $G \times X \longrightarrow X$ such that:

a) $e(x) = x \quad \forall x \in X$.

b) $g_1(g_2(x)) = (g_1 g_2)(x)$ for all $x \in X$ and $g_1, g_2 \in G$.

In other words, it is a homomorphism from G to the permutation group S_X.

2.[10 points] State and prove *only one* of the following theorems: (1) Orbit-Stabilizer Theorem (about relation between orbit of an element x and its stabilizer subgroup), or (2) Factor Theorem (about root of a polynomial).

1) see proof of Thm. 16.16 in the text.

2) See proof of Cor. 23.3 in the text.

3.[20 points] True or false? Justify your answer, that is if true give a short explanation why, if false give a counter-example.

(a) A group G of order 17 has no subgroups except $\{e\}$ and G itself.

True.

Because if $H < G \Rightarrow |H| \mid |G|$

but $|G| = 17$ is prime $\Rightarrow |H| = 1 \Rightarrow H = \{e\}$

or $|H| = 17 \Rightarrow H = G$.

(b) The ring $\mathbb{Z}_n$ is an integral domain for any $n > 0$.

False. $\mathbb{Z}_4$ is not integral domain:

$2 \times 2 = 4 = 0 \pmod 4$

but $2 \neq 0 \pmod 4$.

$\mathbb{Z}_n$ int. domain (in fact field) $\Leftrightarrow$ n is a prime number.

(c) The polynomial ring $\mathbb{Z}_5[x]$ is a finite ring.

False

It contains $x, x^2, x^3, \ldots$

So it is infinite.

(d) The group $\mathbb{Z}_5 \times \mathbb{Z}_5$ is a simple group.

False

$\mathbb{Z}_5 \times \{0\}$ is a subgroup of $\mathbb{Z}_5 \times \mathbb{Z}_5$.

Since $\mathbb{Z}_5 \times \mathbb{Z}_5$ is abelian, all subgroups are normal. So it is not simple.

4.[15 points] Give examples of the following Justify/prove your answer.

(a) A (non-trivial) normal subgroup in the dihedral group D_5 (recall that D_5 is the group of symmetries of a regular pentagon).

The Collection of rotations in D_5 is a subgroup H. It Contains 5 rotations.
So $|H| = 5$. $|D_5| = 2 \times 5 = 10$.
So $[D_5 : H] = 2$. We have already seen that any subgroup of index $\underline{2}$ is automatically normal.

(b) An irreducible polynomial of degree 2 in the ring $\mathbb{Z}_3$.

$x^2 + 1$.

If x^2+1 is not irreducible then it will be factored into product of two degree $\underline{1}$ polynomials, and hence must have a root in $\mathbb{Z}_3$.
But x^2+1 does not have a root as we see by trying $0, 1, 2$.

$0^2 + 1 = 1$
$1^2 + 1 = 2$
$2^2 + 1 = 5 = 2 \pmod 3$.

(c) A group G and a normal subgroup N such that $N \times (G/N)$ is not isomorphic to G.

$G = \mathbb{Z}_4$ $\quad N = \{0, 2\} \cong \mathbb{Z}_2$

$G/N \cong \mathbb{Z}_2$ $\quad \mathbb{Z}_4 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow$ Klein group V

5.[10 points] Let G be a group. For $a \in G$ let $\phi_a(x) = axa^{-1}$. Prove that $a \mapsto \phi_a$ is a homomorphism from G to S_G. Also show that the kernel of this homomorphism is the center $Z(G)$ of G. (Note that S_G is the group of permutations of elements of G, with the operation of composition of permutations.)

We need to show:

$$\forall a,b \in G \implies \phi_{ab} = \phi_a \circ \phi_b$$

$$(\phi_a \circ \phi_b)(x) = \phi_a(\phi_b(x)) = a(bxb^{-1})a^{-1}$$
$$= (ab)\,x\,(b^{-1}a^{-1})$$
$$= (ab)\,x\,(ab)^{-1}$$
$$= \phi_{ab}(x).$$

as required.

$\phi_a \in$ kernel of this homomorphism $\iff \phi_a =$ identity permutation on G

$\iff \phi_a(x) = x \quad \forall x \in G$

$\iff axa^{-1} = x \quad \forall x \in G$

$\iff ax = xa \quad \forall x \in G$

$\iff x \in Z(G)$ (by def. of center $Z(G)$).

6(a).[5 points] Consider the abelian group $G = \mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_2$. Let H be the subgroup $\{(0,0,0),(5,5,1)\}$. Find the order of the element $(1,1,1)+H$ in G/H. Can we find a subgroup K of G such that $(1,1,1)+K$ has order 20 in the factor group G/K?

- The first time a multiple of $(1,1,1)$ lies in H is $5(1,1,1) = (5,5,1) \in H$.

  So order of $(1,1,1)+H$ in G/H is 5.

  (while order of $(1,1,1)$ in G is 10).

- No because order of $(1,1,1)+K$ in G/K is a divisor of $10 =$ order of $(1,1,1)$ in G and hence cannot be 20.

(b).[5 points] Find a subgroup N of the group $G = \mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_2$ such that the element $(1,1,1)+N$ has order 2 in the factor group G/H.

We need to choose N such that $(1,1,1) \notin N$ but $(2,2,2)=(2,2,0) \in N$.

Take $N = \{(0,0,0), (2,2,0), (4,4,0), (6,6,0), (8,8,0)\}$.

7.[10 points] Using definition, prove that

$$R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

is a subring of the field of real numbers $\mathbb{R}$. Show that the element $3 - 2\sqrt{2}$ is a unit element in R (i.e. has multiplicative inverse). Also show that the element $3 + 3\sqrt{2}$ is not a unit in R.

Need to show R is closed under addition and multiplication:

- $(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + (b+d)\sqrt{2} \in R$.

- $(a+b\sqrt{2})(c+d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd$
  $= (ac+2bd) + (ad+bc)\sqrt{2} \in R$.

$(3-2\sqrt{2})(3+2\sqrt{2}) = 3^2 - 4\times 2 = 1$

So $(3+2\sqrt{2}) \in R$ is inverse of $(3-2\sqrt{2})$.

$(3+3\sqrt{2})(3-3\sqrt{2}) = 9 - 9\times 2 = -9$

$\Rightarrow (3+3\sqrt{2})\left(\dfrac{3-3\sqrt{2}}{-9}\right) = 1$

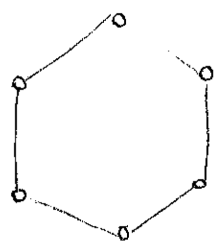
but $\dfrac{3-3\sqrt{2}}{-9} = \left(\dfrac{-3}{9}\right) + \left(\dfrac{3}{9}\right)\sqrt{2} = \left(\dfrac{-1}{3}\right) + \left(\dfrac{1}{3}\right)\sqrt{2} \notin R$

So inverse of $3+3\sqrt{2}$ not in R & hence not a unit in R.

Number of different necklaces =
number of G-orbits $= \frac{1}{12}\left(20+2+2+3\times 4\right) = \frac{36}{12} = \boxed{3}$

8.[15 points] Determine the number of different necklaces that can be made using 3 white beads and 3 black beads. Hint: use group actions and Burnside's theorem.

Let $G = D_6$ act on $X :=$ all possible necklaces with 6 beads
$|G| = 12.$
where 3 are black and 3 are white.



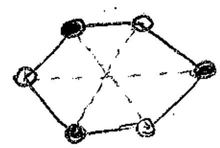
over all there are $\binom{6}{3} = \frac{6\times5\times4}{3\times2\times1} = 20$ elements in X.

For each $g \in G$ we count how many elements in X_g, i.e. how many necklaces fixed by g:

g = rotation $\underline{0}$ degrees : $|X_g| = |X| = 20$

g = " $\underline{60}$ " : none

g = " $\underline{120}$ " :



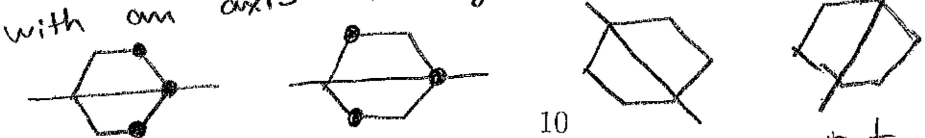
$|X_g| = 2.$

g = " $\underline{180}$ " : none

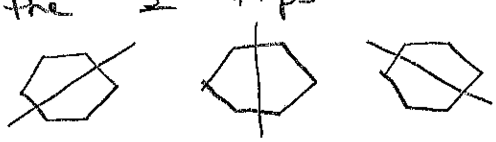
g = " -120 " : $|X_g| = 2$

g = " -60 " : none

g = any of the $\underline{3}$ flips (reflections) with an axis through one of the $\underline{6}$ beads: $|X_g| = 4$



g = any of the $\underline{3}$ flips with axis not through beads: none



9.[2 points] Draw yourself taking this exam!