NOTE TO PRINTER

(These instructions are for the printer. They should not be duplicated.)

THIS EXAMINATION SHOULD BE PRINTED ON $8\frac{1}{2} \times 14$ PAPER, AND STAPLED WITH 3 SIDE STAPLES, SO THAT IT OPENS LIKE A LONG BOOK.

McGILL UNIVERSITY
FACULTY OF SCIENCE
FINAL EXAMINATION

MATHEMATICS 189–340B

ABSTRACT ALGEBRA AND COMPUTING

EXAMINER: Professor W. G. Brown DATE: Monday, April 19th, 1999
ASSOCIATE EXAMINER: Professor J. Loveys TIME: 14:00 – 17:00 hours

SURNAME: SEAT NO.:
MR, MISS, MS, MRS, &c.:
GIVEN NAMES:

STUDENT NUMBER: COURSE AND YEAR:

Instructions

1. Fill in the above clearly.
2. Do not tear pages from this book; all your writing — even rough work — must be handed in.
3. Calculators are not permitted.
4. This examination booklet consists of this cover, Pages 1 through 9 containing questions; and Pages 10 and 11, which are blank.
5. Show all your work. All solutions are to be written in the space provided on the page where the question is printed. When that space is exhausted, you may write *on the facing page*. Any solution may be continued on the last pages, or the back cover of the booklet, but you must indicate any continuation clearly on the page where the question is printed!
6. You are advised to spend the first few minutes scanning the problems. (Please inform the invigilator if you find that your booklet is defective.)

PLEASE DO NOT WRITE INSIDE THIS BOX

1(a) /5	1(b) /5	2 /10	3 /10	4(a) /7	4(b) /8	5 /10	6 /10
7(a) /4	7(b) /6	8(a) /7	8(b) /8	9(a) /5	9(b) /5		
				Raw /	Scaled /	TERM /	

1. (a) [5 MARKS] Prove or disprove: If $(\mathfrak{A}, *, e)$ is any group, the function $f : \mathfrak{A} \to \mathfrak{A}$ defined by $a \mapsto a^2$ is a homomorphism.

   (b) [5 MARKS] Prove or disprove: The order of every subgroup of S_5 is divisible by 5.

2. [10 MARKS] Showing all your work, determine all integer solutions to the system of congruences

$$\begin{aligned} x &\equiv 5 \pmod{74} \\ x &\equiv 19 \pmod{22} \end{aligned}$$

(Where inverses are required to a modulus exceeding 10, they should be found using the Euclidean Algorithm — not by inspection.)

3. [10 MARKS] Showing all your work, *carefully* determine all positive integers n such that $\phi(n) = 4$, where ϕ is the Euler totient function.

4. (a) [7 MARKS] Prove that the polynomial $1 + x + x^3$ is irreducible over $\mathbb{Z}_2$.

(b) [8 MARKS] Using the polynomial $1 + x + x^3$ to construct a field of order 8, show the multiplication table of that field.

5. Suppose that $*$ is a binary operation on a set $\mathfrak{A}$, having the following properties:

$$(\exists b)(\forall c)[c * b = c = b * c]$$

$$(\forall x)(\forall y)(\forall z)[x * (y * z) = (x * z) * y]$$

where the universe for all quantifiers $\exists$, $\forall$ is $\mathfrak{A}$. Showing <u>all</u> your work, determine carefully

(a) [6 MARKS] whether $*$ is associative.

(b) [4 MARKS] whether $*$ is commutative.

6. [10 MARKS] Describe 5 groups of order 36, no two of which are isomorphic. You are expected to prove that no two of your 5 groups are isomorphic.

7. (a) [4 MARKS] Prove or disprove: $\mathbb{Z}_6$ is a field.

(b) [6 MARKS] Prove or disprove: In the ring $\mathbb{R}\{x\}$ of formal power series with real coefficients, the only element which has no multiplicative inverse is 0 (i.e. the power series $0x^0 + 0x^1 + 0x^2 + \ldots + 0x^n + \ldots$).

8. (a) [7 MARKS] Prove that, for any integers a and n both greater than 1, $a^{4n} + a^{2n} + 1$ is composite.

(b) [8 MARKS] Showing all your work, determine a non-negative integer a such that $a \equiv 3^{50000} \pmod{3^4+3^2+1}$ and $0 \leq a < 100$. You are expected to carry out these calculations by hand, and to use techniques which do not require working with large integers (with the exception of the exponent 50,000).

9. (a) [5 MARKS] For the element $a = (13)$ of the permutation group whose set of elements is $\{e, (12), (13), (23), (123), (132)\}$, determine the right translation R_a and the left translation L_a, and express them both as permutations of the group elements, in disjoint cycle notation.

(b) [5 MARKS] Give an example of a right coset of $\langle (23)(14) \rangle$ in A_4 which is not a left coset of $\langle (14)(23) \rangle$ in A_4; or prove that no such example exists.

CONTINUATION PAGE FOR PROBLEM NUMBER □

You *must* refer to this continuation page on the page where the problem is printed!

CONTINUATION PAGE FOR PROBLEM NUMBER □

You *must* refer to this continuation page on the page where the problem is printed!