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
SUPPLEMENTAL/DEFERRED EXAMINATION

MATHEMATICS 189–340B

ABSTRACT ALGEBRA AND COMPUTING

EXAMINER: Professor W. G. Brown DATE: Wednesday, AUGUST ??th, 2002
ASSOCIATE EXAMINER: Professor W. O. J. Moser TIME: 09:00 – 12:00 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 7 containing questions; and Pages 8 and 9, 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 <u>must</u> 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) /6	1(b) /6	2 /12	3 /16	4 /12	5 /16	6(a) /12	6(b) /4
7(a) /12	7(b) /4						

1. (a) [6 MARKS] Consider the set $S = \mathbb{Z} - \{0\}$. Prove or disprove the following statement: S is a group under the usual operation of multiplication in $\mathbb{Z}$.

   (b) [6 MARKS] Let R be a ring containing a multiplicative identity 1_R, and suppose that $0_R = 1_R$. Showing all your work, determine the cardinality $|R|$ of R.

2. [12 MARKS] Use properties of congruences to prove that, for any positive integer n, $3^{2(4n+1)} + 2^{3(4n+1)}$ is a multiple of 17. [Hint: $9 + 8 \equiv 0 \pmod{17}$.]

3. [16 MARKS] Describe four groups of order 24, no two of which are isomorphic. For all pairs of these groups you are expected to explain precisely how you know they are not isomorphic.

4. [12 MARKS] Carefully showing all your work, determine all integers that satisfy all of the following congruences simultaneously:

$$x \equiv -11 \pmod 7 \tag{1}$$
$$x \equiv -7 \pmod{11} \tag{2}$$
$$x \equiv -2 \pmod 2 \tag{3}$$

Should you require the inverse to a given modulus n of an integer which is different from both 1 and -1, you are expected to use only the Euclidean algorithm to find it.

5. [16 MARKS] In the ring $\mathbb{Z}_3[x]$ let $f(x) = x^3+x+1$, $g(x) = x^4+x^3+1$. Showing all your work, determine polynomials $a(x)$ and $b(x)$ such that

$$(f(x), g(x)) = f(x) \cdot a(x) + g(x) \cdot b(x) \,.$$

6. (a) [12 MARKS] Showing all your work, determine the right coset decomposition with respect to the subgroup

$$H = \{e, (12), (24), (14), (124), (214)\}$$

of the group S_4 of all permutations of the set $\{1, 2, 3, 4\}$.

(b) [4 MARKS] By referring to the subgroup H of S_4 in the previous subquestion show that a right coset need not be a left coset.

7. (a) [12 MARKS] Showing all your work, determine all irreducible polynomials of degree 3 over the field $\mathbb{Z}_2$. All your work must be shown neatly, and you are not to quote any polynomials from memory.

   (b) [4 MARKS] Prove or disprove: If $f(x)$ is a polynomial that is irreducible over $\mathbb{Z}_2$, then $f(x^2)$ cannot be irreducible.

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!