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: .....day, August ..th, 2001
ASSOCIATE EXAMINER: Professor W. O. J. Moser — TIME: ..:00 – ..: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 6 containing questions; and Pages 7 and 8, 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) /6	4(b) /6	4(c) /6	5 /12
6(a) /5	6(b) /5						
				RAW /70	SCALED /100	TERM /30	

1. Suppose that f is a homomorphism from ring $\mathcal{R}$ to ring $\mathcal{S}$, and that the *kernel* of f consists only of the zero element of $\mathcal{R}$. Prove or disprove each of the following statements:

   (a) [5 MARKS] $\mathcal{R}$ must be commutative.

   (b) [5 MARKS] f must be surjective.

2. [10 MARKS] Showing all your work, determine all positive integers n such that $\varphi(2n) = \varphi(n)$ (where φ is the Euler *totient* function).

3. [10 MARKS] Carefully showing all your work, determine all integers that satisfy all of the following congruences simlutaneously:

$$
\begin{aligned}
x &\equiv -28 \pmod 3 && (1)\\
x &\equiv 13 \pmod 5 && (2)\\
x &\equiv 70 \pmod{11} && (3)\\
x &\equiv 1000 \pmod 8 && (4)
\end{aligned}
$$

(Should you require the inverse of an integer n to a given modulus, you should use a systematic method to find it, unless $n = \pm 1$.)

4. (a) [6 MARKS] Showing all your work, prove carefully that the polynomial $x^4 + x + 1$ is irreducible over $\mathbb{Z}_2$, but is reducible over $\mathbb{Z}_5$.

   (b) [6 MARKS] Discuss in detail how one can use the polynomial $x^4 + x + 1$ to construct a field $\mathbb{F}_{16}$ of order $2^4 = 16$. Show the inverses of at least 2 of the elements of the field.

   (c) [6 MARKS] Carefully determine the order of the element x^5 in the multiplicative group of the field that you have constructed.

5. [12 MARKS] Recall that the symmetric group S_n consists of all permutations f of the set $\{1, 2, ..., n\}$. Determine, in $\mathcal{S}_4$, all cosets of the subgroup H which is generated by the permutation (4321). You are expected to show the precise membership of each of the cosets.

6. Let a relation $\sim$ on the set $\mathbb{Z} - \{0\}$ be defined as follows:

$$a \sim b \quad \Leftrightarrow \quad (\forall n \in \mathbb{Z} - \{0\})\,(n|a \Rightarrow (n+1)|b)\,.$$

   (a) [5 MARKS] Determine whether or not $\sim$ is an equivalence relation.

   (b) [5 MARKS] Determine whether or not $\sim$ is a partial ordering of $\mathbb{Z} - \{0\}$.

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!