McGill University December 2012
Faculty of Science Final Examination

Abstract Algebra

Math 235

Monday December 10, 2012

Time: 9:00 am - 12:00 pm

Examiner: Prof. Henri Darmon Associate Examiner: Prof. Eyal Goren

INSTRUCTIONS

1. Please answer questions in the exam booklet provided.
2. This exam consists of 10 questions. Each question is worth 10 points.
3. This a CLOSED BOOK exam. No notes, textbooks or crib sheets are permitted.
4. Calculators, cell phones, smart phones, tablets and laptops are not permitted.
5. Please write your name clearly on the examination booklet.

This exam comprises the cover page and two page of questions.

1. Let $f(x)$ and $g(x)$ be non-zero polynomials in the ring $F[x]$ of polynomials with coefficients in a field F. Let L be the set of all *non-zero* linear combinations of f and g:

$$L = \{a(x)f(x) + b(x)g(x), \text{ with } a, b \in F[x] \text{ and } af + bg \neq 0.\}.$$

(a) Let $h(x)$ be a monic polynomial in L of minimal degree. Show that $h(x)$ divides both $f(x)$ and $g(x)$.
(b) Show that this polynomial $h(x)$ is the gcd of $f(x)$ and $g(x)$.

2. Let $R = \mathbf{Z}[x]$ be the ring of polynomials with coefficients in $\mathbf{Z}$. Show that the ideal

$$I = (2, x^2 + x + 1) = \{2f(x) + (x^2 + x + 1)g(x), \quad \text{with } f, g \in \mathbf{Z}[x] \ \}$$

generated by 2 and $x^2 + x + 1$ is not a principal ideal. Show that the quotient R/I is a field. How many elements does it contain?

3. Let (a_n) be a sequence of integers defined recursively by the rules

$$a_0 = 14, \qquad a_1 = 21, \qquad a_{n+1} = 5a_n + a_{n-1}.$$

What is the gcd of a_{1000} and a_{1001}? You should prove that your answer is correct.

4. Let $F = \mathbf{Z}/p\mathbf{Z}$ be the field with p elements, where p is a prime. Show that the polynomial $x^{p-1} - 1$ admits the factorisation

$$x^{p-1} - 1 = (x - 1)(x - 2) \cdots (x - (p - 1))$$

in $F[x]$. State Wilson's theorem and derive it from the above polynomial identity.

5. Let $n = 1729 = 7 \times 13 \times 19$ and let a be any integer satisfying $\gcd(a, n) = 1$. Show that $a^{n-1} \equiv 1 \pmod{n}$.

6. Show that the ring

$$\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5}, \quad \text{with } a, b \in \mathbf{Z}\}$$

is not a unique factorisation ring by factoring the number 6 into irreducible elements in this ring in two fundamentally distinct ways.

7. Write down the elements in the alternating group $G = A_4$ on 4 letters, using cycle notation. Write down the cosets in G/H and in $H\backslash G$ where H is the subgroup of G given by

$$H = \{1, (12)(34), (13)(24), (14)(23)\}.$$

Using this calculation, show that H is a normal subgroup of G. What is the quotient G/H isomorphic to?

8. Let G be a finite group. Show that the order of any element in G divides the cardinality of G. Explain how this fact can be used to prove Fermat's Little Theorem.

9. Let $G = \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ be a product of two cyclic groups of order 3. Show that G cannot be (isomorphic to) a subgroup of the multiplicative group $(\mathbf{Z}/p\mathbf{Z})^\times$, where p is a prime number. (Hint: consider the polynomial $x^3 - 1$ in $\mathbf{Z}/p\mathbf{Z}[x]$.)

10. Let m and n be two integers that are relatively prime, and let

$$f : \mathbf{Z} \longrightarrow \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$$

be the homomorphism sending the integer a to the pair $(a \pmod{m}, a \pmod{n})$. What is the kernel of f? Explain why this can be used, in conjunction with the first isomorphism theorem for rings, to conclude the Chinese remainder theorem.