Department of Mathematics
MA/PhD Qualifying Examination
in Algebra

Examiners: Wee Teck Gan, Philip Gill and Cristian Popescu

10:00am–1:00pm, AP&M 7421
Wednesday May 31, 2006

NAME ____________________

#1.1	20	
#1.2	20	
#2.1	20	
#2.2	20	
#3.1	25	
#3.2	30	
#3.3	25	
#4.1	20	
#4.2	20	
Total	200	

- Do all problems.
- Add your name in the space provided and staple this page to your solutions for Section #1.
- Start your solutions for the questions in Sections #2 and #4 on a fresh page.
- Write your name clearly on every sheet submitted.

1. Linear Algebra

Question 1.1.

(a) Consider $\lambda_i, \lambda_j \in \text{eig}(A)$ such that $\lambda_i \neq \lambda_j$. Let (x_i, y_i) and (x_j, y_j) denote the right and left eigenvectors of A associated with λ_i and λ_j. Show that $y_i^* x_j = 0$.

(b) Let x denote an eigenvector of A associated with an eigenvalue λ. Prove that if λ has a left-eigenvector y such that $y^* x = 0$, then $\text{am}(\lambda) > 1$.

Question 1.2. Given $A \in M_{m,n}$ with $m \geq n$, prove that there exists a unique $U \in M_{m,n}$ with orthonormal columns, and a unique Hermitian positive semidefinite $H \in M_n$ such that $A = UH$.

(*State in detail any auxiliary results used without proof.*)

2. Group Theory

Question 2.1. Let p be a prime number.

(a) Show that the order of $\widehat{1+p}$ in $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is equal to p.

(b) Use (a) above to construct a non-abelian group of order p^3.

(c) Describe the non-abelian group you have constructed in (b) above via generators and relations.

Note. As usual, $(\mathbb{Z}/p^2\mathbb{Z})^\times$ denotes the multiplicative group consisting of all the congruence classes $\widehat{x} \in \mathbb{Z}/p^2\mathbb{Z}$, such that $\gcd(x, p) = 1$.

Question 2.2. Let G be a group. Let $r \geq 2$ be an integer. Assume that G contains a non-trivial subgroup H of index $[G : H] = r$. Prove the following.

(a) If G is simple, then G is finite and $|G|$ divides $r!$.

(b) If $r \in \{2, 3, 4\}$, then G cannot be simple.

(c) For all integers $r \geq 5$, there exist simple groups G which contain non-trivial subgroups H of index $[G : H] = r$.

3. Ring Theory and Module Theory

Question 3.1. Let $f \in \mathbb{Z}[X] \setminus \mathbb{Z}$, such that $\gcd(f, f') = 1$. Let S be the set of non-zero divisors in the quotient ring $\mathbb{Z}[X]/(f)$.

(a) Show that the ring $S^{-1}(\mathbb{Z}[X]/(f))$ is isomorphic to a direct sum of fields.

(b) Specify the fields in (a) above if $f = X^5 - 1$.

(c) Is the hypothesis $\gcd(f, f') = 1$ necessary in order for the conclusion in (a) above to hold true ? Justify.

Note. As usual, if $f = a_n X^n + \cdots + a_1 X + a_0$ is a polynomial in $\mathbb{Z}[X]$, then f' denotes the formal derivative of f in $\mathbb{Z}[X]$, given by $f' = n a_n X^{n-1} + \cdots + a_1$. Also, $\gcd(f, f')$ denotes the greatest common divisor of f and f' in $\mathbb{Z}[X]$.

Question 3.2. Let R be a commutative ring and let M and N be R–modules. Prove the following.

(a) If M and N are projective R–modules, then $M \otimes_R N$ is a projective R–module.

(b) If M and N are flat R–modules, then $M \otimes_R N$ is a flat R–module.

(c) If M is a flat R–module and N is an injective R–module, then $\mathrm{Hom}_R(M, N)$ is an injective R–module.

(d) Let p be a prime number and let $\mathbb{Z}_{(p)}$ denote the localization of $\mathbb{Z}$ with respect to its prime ideal $p\mathbb{Z}$. Show that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_{(p)}, \mathbb{Q}/\mathbb{Z})$ is an injective $\mathbb{Z}$–module.

Question 3.3. Let n be a squarefree integer greater than 3. Let R denote the subring $\mathbb{Z}[\sqrt{-n}] = \{a + b\sqrt{-n} \mid a, b \in \mathbb{Z}\}$ of the field of complex numbers $\mathbb{C}$.

(a) Show that $\sqrt{-n}$ and $1 + \sqrt{-n}$ are irreducible in R.

(b) Prove that R is not a unique factorization domain (UFD).

(c) Construct an ideal in R which is not principal.

Hint. In a UFD, an element is irreducible if and only if it is prime.

4. Field Theory and Galois Theory

Question 4.1.

(a) If $\mathbb{F}_q$ is a finite field with q elements, show that $\mathbb{F}_q^\times$ is a cyclic group.

(b) Show that for each integer $n \geq 1$, there exists an irreducible polynomial over $\mathbb{F}_q$ of degree n.

(c) Consider the map $\phi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ given by $\phi(x) = x^q$. Note that ϕ is an $\mathbb{F}_q$-linear endomorphism of the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^n}$. Find the characteristic and minimal polynomials of ϕ.

Question 4.2.

(a) Let p be an odd prime. Show that $\sin(\frac{2\pi}{p})$ is algebraic over $\mathbb{Q}$ and determine its degree over $\mathbb{Q}$.

(b) Show that $\mathbb{Q}(\sin(\frac{2\pi}{p}))$ is a Galois extension of $\mathbb{Q}$ and determine its Galois group over $\mathbb{Q}$.

(c) Find all p's such that $p^{1/3} \in \mathbb{R}$ is contained in $\mathbb{Q}(\sin(\frac{2\pi}{p}))$.