# Math 4320 : Introduction to Algebra

**Final Exam**

(May 15, 2009, 2-4pm)

Books and calculators are not allowed.

**1. (basic notions in group theory)**

**(a) (5 pts)** Is $D_{2n}$ an abelian (commutative) group? How about $S_n$? (Your answer might depend on $n$.)

$D_{2n}$ and $S_n$ are abelian only for $n = 2$.

**(b) (5 pts)** Define a simple group and give an example. (Giving the symbol of the group is not sufficient. Describe the group you suggest.)

A simple group is a group of which there is no normal subgroup other than $\{1\}$ and itself. An example is the group of even permutations $A_5$ on five letters.

**(c) (5 pts)** Is every finite group isomorphic to a subgroup of $S_n$ for some $n$? Explain your answer.

Yes, by Cayley theorem, since a finite group $G$ acts on itself by conjugation.

**2. (group isomorphism)**

**(a) (7 pts)** Prove that no pair of the following groups of order 8 are isomorphic:

$$\mathbb{I}_8, \quad \mathbb{I}_4 \times \mathbb{I}_2, \quad \mathbb{I}_2 \times \mathbb{I}_2 \times \mathbb{I}_2, \quad D_8.$$

$D_8$ is non-isomorphic to the rest because it is non-abelian (where are all the others are). Among the rest, $I_8$ is the only group having an element of order 8, thus non-isomorphic to the rest. We are left with two groups : $I_4 \times I_2$ has an element of order 4, but $I_x^3$ does not, so they are non-isomorphic.

**(b) (8 pts)** Prove that $\mathbb{I}_6$ is isomorphic to $\mathbb{I}_2 \times \mathbb{I}_3$.

Define a homomorphism $\mathbb{Z} \to I_2 \times I_3$, by sending $a \mapsto ([a]_2, [a]_3)$. It is clearly well-defined, and it is a surjective homomorphism since it is a product of projections. The kernel is the set of elements which are zero modulo 2 and zero modulo 3, thus $6\mathbb{Z}$. By the first isomorphism theorem, $I_6 = \mathbb{Z}/6\mathbb{Z}$ is isomorphic to $I_2 \times I_3$.

**3. (class equation) (5 pts each)** Find the class equation $|G| = |Z(G)| + \sum [G : C_G(x)]$ of

**(a)** the four group $V$,

The group $V$ is abelian, thus $4 = 4$ is the class equation.

**(b)** the symmetric group $S_3$.

**4. (basic notions in rings and fields) (5 pts each)**

**(a)** Describe elements of each of the field $Frac(R[x])$ and the field $(Frac(R))(x)$? Are they isomorphic? Why?

Elements of $Frac(R[x])$ are of the form $f/g$ where $f, g$ are polynomials with coefficients in $R$. The elements of $(FracR)(x)$ are of the form $f/g$ where $f, g$ are polynomials with coefficients in $Frac(R)$. They are isomorphic. The first field is clearly a subset of the second field, and by multiplying by the common denominator of coefficients of $f, g$ the second field is also contained in the first field.

**(b)** Give an example of a field which is not a set of numbers (nor a set of equivalence classes of numbers).

The field $\mathbb{Q}[x]$ of rational functions $f/g$ of polynomials $f, g$ in $\mathbb{Q}[x]$.

**5. (field isomorphisms)(5 pts each)**

**(a)** Explain why a field of order 4 and $\mathbb{I}_4$ are not isomorphic (as rings).

Because one is a field and the other is not : $I_4 = \mathbb{Z}/4\mathbb{Z}$ is not a field since $4\mathbb{Z}$ is not a maximal ideal ($2\mathbb{Z}$ is a maximal ideal containing it).

**(b)** Are $\mathbb{F}_3[x]/(x^2+1)$ and $\mathbb{F}_3[x]/(x^2+x-1)$ isomorphic as fields? Why?

Yes, because there is a unique field for each order, and they have the same order since they are both vector spaces of dimension 2 over $\mathbb{F}_3$.

**6. (Irreducibles)(10 pts each)**

**(a)** List all the irreducible polynomials in $\mathbb{F}_2[x]$ of degree less than or equal to 3. (First list all polynomials and show your process of elimination.)

All polynomials : $x, x+1, x^2, x^2+x, x^2+x+1, x^2+1, x^3, x^3+x^2, x^3+x^2+x, x^3+x, x^3+x^2+x+1, x^3+x, x^3+x+1, x^3+x^2+1$.

All irreducible polynomials : $x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1$.

**(b)** Show that the $p$-th cyclotomic polynomial $x^{p-1}+x^{p-2}+\cdots+x+1$ is an irreducible polynomial in $\mathbb{Q}[x]$.

The polynomial $\Phi_p(x) = (x^p-1)/(x-1)$. Since $\Phi_p(x+1) = [(x+1)^p - 1]/x = x^{p-1} + ... + p$ where all the intermediate coefficients are divisible by $p$. By Eisenstein criterion, it is irreducible in $\mathbb{Q}[x]$, thus so is $\Phi_p(x)$.

**7. (fields and domains)(5 pts each)** Let $R$ be the ring $R = \mathbb{Z}[\theta] = \{a + b\theta : a, b \in \mathbb{Z}\}$, where $\theta = \frac{1+\sqrt{-19}}{2}$.

**(a)** Define $N(a+b\sqrt{-19}) = a^2+19b^2$. Show that $\pm 1$ are the only units in $R$. (Hint : Use the fact that $N$ is multiplicative, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$.)

If $u$ is a unit, $N(u) = 1$. Thus $a = \pm 1$ and $b = 0$.

**(b)** What is the fraction field $F = Frac(R)$ of $R$? What is the prime field of $F$?

The fraction field is $\mathbb{Q}[\sqrt{-19}] = \{a + b\sqrt{-19} : a, b \in \mathbb{Q}$. The prime field is $Q$.

**8. (prime ideals and maximal ideals)(5 pts each)**

**(a)** Given an example of a prime ideal $I$ in $\mathbb{Z}[x]$.

$(x)$.

**(b)** Is your example $I$ in part (a) a maximal ideal? If not, find a maximal ideal containing $I$.

No. The maximal ideal containing $x$ is the set of all polynomials such that the constant coefficient is even. It is maximal since the quotient is isomorphic to the field $\mathbb{F}_2$.

**(c)** Show that if $R$ is a PID, then every nonzero prime ideal $I$ is a maximal ideal.

**9. (field automorphism)(5 pts each)** Let $E = \mathbb{Q}(\xi_5)$ be the field obtained from $\mathbb{Q}$ by adjoining $\xi_5 = e^{2\pi i/5}$.

**(a)** Find an automorphism of $F$ fixing $\mathbb{Q}$.

The map fixing $\mathbb{Q}$ and sending $\xi_5$ to $\xi_5^2$.

**(b)** What is the dimension of $F$ as a vector space over $\mathbb{Q}$? Find a basis of $F$ over $\mathbb{Q}$.

A polynomial having $\xi_3$ as a root is $x^5 - 1$. An irreducible polynomial having $\xi_3$ as a root is $x^4 + x^3 + x^2 + x + 1$. $\{1, \xi, \xi^2, \xi^3\}$ is a basis, and the dimension is 4.

**(c)** Find a principal ideal $I$ such that the field $\mathbb{Q}[x]/I$ is isomorphic to $E$.

The ideal generated by $x^4 + x^3 + x^2 + x + 1$.

**Extra problem A. (1 pt)** State Galois Theorem (in Galois Theory). Outline the proof of “insolvability of the general quintic polynomials” using Galois Theorem.

**Extra problem B. ($\epsilon$ pt)** State the most interesting theorem you learned in this course.