

**THE JOHNS HOPKINS UNIVERSITY**  
**Faculty of Arts and Sciences**  
**FINAL EXAM - SPRING SESSION 2006**  
**110.402 - ADVANCED ALGEBRA II.**

Examiner: Professor C. Consani  
Duration: 3 HOURS (9am-12:00pm), May 15, 2006.

No calculators allowed.

Total Marks = 100

**SOLUTIONS**

1. [20 marks]

(1) Let  $n, m$  be two positive integers. Give an explicit description of the set

$$\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$$

as an abelian group, i.e. determine its structure as abelian group.

(2) Let  $f(X) \in \mathbb{Z}[X]$  be a monic polynomial of degree  $n > 0$ . Show or disprove the following statement:

$$\mathbb{Z}[X]/(f(X)) \text{ is a free abelian group of rank } n$$

### Solution

(1) First notice that a homomorphism  $\varphi : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$  is determined by the image of 1 (the image of any other element is recovered by additivity). Moreover, the order of  $\varphi(1)$  in  $\mathbb{Z}/m\mathbb{Z}$  divides  $n$  since

$$n\varphi(1) = \varphi(n) = \varphi(0) = 0.$$

The elements of  $\mathbb{Z}/m\mathbb{Z}$  whose orders divide  $n$  form a subgroup generated by

$$a = m/\text{gcd}(m, n)$$

(If  $nx$  is divisible by  $m$ , then  $nx/\text{gcd}(m, n)$  is divisible by  $a$ , and since  $n/\text{gcd}(m, n)$  and  $a$  are coprimes,  $x$  is divisible by  $a$ ). All these elements clearly correspond to homomorphisms from  $\mathbb{Z}/n\mathbb{Z}$  to  $\mathbb{Z}/m\mathbb{Z}$ . Hence  $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$  is a cyclic group with  $\text{gcd}(m, n)$  elements.

(2) The statement is true. Denote by  $y$  the image of  $X$  in  $R = \mathbb{Z}[X]/(f(X))$ . The ring  $R$  is generated by  $1, y, y^2, \dots, y^{n-1}$ , since  $y^n$  is a linear combination of these elements with integral coefficients. Let us show that  $\{1, y, \dots, y^{n-1}\}$  forms a free basis of  $R$ . Assume the contrary: i.e. there is a relation

$$a_0 + a_1y + \dots + a_{n-1}y^{n-1} = 0$$

This means that the polynomial  $a_0 + a_1X + \dots + a_{n-1}X^{n-1}$  is divisible by  $f(X)$ , which is impossible since the latter has higher degree.

2. [20 marks]

- (1) Let  $K$  be an algebraic extension of a field  $k$ . Prove, or find a counterexample to the following statement:

if  $A$  is a ring and  $k \subset A \subset K$ , then  $A$  is a field.

[Hint: Use the definition of an algebraic element as a root of a (monic) polynomial]

- (2) Is

$$\alpha = \frac{3 + 2\sqrt{6}}{1 - \sqrt{6}}$$

an algebraic integer? Explain your answer in details.

Determine  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$  and if  $\mathbb{Q}(\alpha)$  is a  $\mathbb{Q}$ -algebraic extension, find its minimal polynomial.

### Solution

- (1) The statement is true. We need only show that every nonzero element of  $A$  has an inverse in  $A$  to show that  $A$  is in fact a field. So let  $a \in A$  be a nonzero element. There exists  $b \in K$  such that  $ab = 1$ , and we want to show that  $b \in A$ .

Since  $K$  is an algebraic extension of  $k$ ,  $b$  is algebraic over  $k$ , so  $b$  is the root of a polynomial over  $k$ . Let

$$m_{b,k}(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 \in k[x]$$

be the minimal polynomial of  $b$  over  $k$ , where  $n \geq 1$ . Then  $m_{b,k}(b) = 0$ , and hence  $-a^{n-1}m_{b,k}(b) + b = b$ . But  $-a^{n-1}m_{b,k}(b) + b = -c_{n-1} + \cdots + (-a^{n-2}c_1) + (-a^{n-1}c_0) \in A$  since  $ab = 1$ , which shows that  $b \in A$ .

- (2) We have

$$\alpha = \frac{3 + 2\sqrt{6}}{1 - \sqrt{6}} = \frac{(3 + 2\sqrt{6})(1 + \sqrt{6})}{-5} = -3 - \sqrt{6}.$$

Since  $(\alpha + 3)^2 = 6$ , the number  $\alpha$  is an algebraic integer. As  $\sqrt{6}$  is irrational the polynomial  $(x + 3)^2 - 6$  is irreducible, hence it is the minimal polynomial of  $\alpha$  and  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ .

3. [20 marks]

- (1) Let  $K_f$  be the splitting field of the polynomial

$$f(x) = x^3 - 3x^2 + 1 \in \mathbb{Z}[X].$$

Determine the group  $\text{Gal}(K_f/\mathbb{Q})$ .

Find all proper extensions of  $\mathbb{Q}$  contained in  $K_f$ .

- (2) Is there any relation connecting the Galois groups of the following two rational polynomials

$$f(x) = x^{12} - 1, \quad g(x) = x^2 - 3 ?$$

Explain in details your answer.

### Solution

- (1) The polynomial  $f(x)$  is irreducible (enough to check that  $\pm 1$  are not roots since any integral root should divide the free term). The discriminant

$$D = -4 \cdot (-3)^3 - 27 \cdot (-1)^2 = 81$$

is a full square. Hence the Galois group is  $A_3$  (the only proper transitive subgroup of  $S_3$ ). There are no nontrivial subgroups of  $A_3$ . Thus there are no nontrivial subextensions of  $K_f/\mathbb{Q}$ .

- (2) Denote by  $K_f$  and  $K_g$  the splitting fields of  $f$  and  $g$  respectively. The roots of  $g(x)$  are  $\pm\sqrt{3}$ . These roots belong to  $K_f$  since  $\sqrt{3} = \zeta + \zeta^{-1}$  where  $\zeta = \frac{\sqrt{3}}{2} + \frac{i}{2}$  is a primitive 12-th root of 1. So  $K_g \subset K_f$ . The extension  $K_g/\mathbb{Q}$  is Galois hence  $\text{Gal}(K_g/\mathbb{Q})$  is a quotient group of  $\text{Gal}(K_f/\mathbb{Q})$ .

4. [20 marks] Let  $K = \mathbb{Q}(\zeta_{17})$ , where  $\zeta_{17}$  is a primitive 17th root of 1.

How many proper extensions of  $\mathbb{Q}$  are contained in  $K$ ?

Does  $K$  contain any real field? If yes, give an explicit description of at least one of these fields.

Show that the discriminant  $D_f$  of the polynomial  $f(x) = x^{17} - 1$  verifies

$$D_f = \prod_{i=0}^{16} f'(\zeta_{17}^i), \quad f'(x) = \frac{d}{dx} f(x).$$

Deduce the existence of a quadratic extension of  $\mathbb{Q}$  contained in  $K$ . Describe it explicitly.

Are there any further quadratic extensions of  $\mathbb{Q}$  contained in  $K$ ? Why?

### Solution

The Galois group  $\text{Gal}(K/\mathbb{Q})$  is the cyclic group of order 16 (=the multiplicative group of all invertible elements in  $\mathbb{Z}/17\mathbb{Z}$ ). For each  $a$  that divides 16 there is a unique subgroup of order  $a$ . There are 3 proper divisors of 16 (namely, 2, 4 and 8) so we have 3 proper sub-extensions of  $K/\mathbb{Q}$ .

The number  $w = \zeta_{17} + \zeta_{17}^{-1}$  is real and irrational. The field  $\mathbb{Q}(w)$  is a nontrivial real subfield of  $K$ .

Given a polynomial  $f(x) = \prod_{i=1}^n (x - x_i)$  ( $x_i$  are the roots of  $f$  in its splitting field) the discriminant  $D_f$  is defined as  $\prod_{i < j} (x_i - x_j)^2$ . Note that  $f'(x_i) = \prod_{x_j \neq x_i} (x_i - x_j)$ . Therefore

$$\prod_{i \neq j} f'(x_i) = \prod_{i \neq j} (x_i - x_j) = (-1)^{n(n-1)/2} \prod_{i < j} (x_i - x_j)^2 = (-1)^{n(n-1)/2} D_f.$$

In our case  $(-1)^{n(n-1)/2} = 1$  (since  $n = 16$  is divisible by 4). By the above formula,  $D_f = 17^{17} \zeta^{16(1+2+\dots+16)} = 17^{17}$ . So  $\mathbb{Q}(\sqrt{D_f}) = \mathbb{Q}(\sqrt{17})$  is a quadratic subextension of  $K$ . A quadratic sub-extension is unique (there is a unique subgroup of index 2 in the cyclic group with 16 elements).

5. [20 marks]

- (1) Let  $\mathbb{F}_4$  be the finite field with 4 elements. Consider the map:

$$\sigma : \mathbb{F}_4 \rightarrow \mathbb{F}_4, \quad \sigma(x) = x^3$$

Does this map define an automorphism of  $\mathbb{F}_4$ ? Explain your answer. If not, define a homomorphism of  $\mathbb{F}_4$  that is an automorphism. How many automorphisms do we expect?

- (2) Consider the polynomial

$$f(X) = X^8 - X \in \mathbb{F}_2[X].$$

Let  $K$  be the splitting field of  $f(X)$ .

Determine  $[K : \mathbb{F}_2]$  and the cardinality of the multiplicative group of units  $K^\times$ .

Is  $\mathbb{F}_4$  a sub-field of  $K$ ? Explain.

**Solution**

- (1) The multiplicative group  $\mathbb{F}_4^\times$  has order 3. Therefore for each nonzero element  $a \in \mathbb{F}_4$  we have  $a^3 = 1$ . It follows that  $\sigma$  is not 1-1 and hence is not an automorphism.

To get an automorphism it is enough to take  $\phi(x) = x^2$  (we have  $(x + y)^2 = x^2 + 2xy + y^2 = x^2 + y^2$  since the  $\text{char}(\mathbb{F}_4) = 2$ ). Each automorphism must preserve 0 and 1. So it can either interchange the remaining 2 elements or leave them fixed. Hence there are only 2 automorphisms of  $\mathbb{F}_4$ :  $\text{id}$  and  $\phi$  (it is easy to see that  $\phi \neq \text{id}$  — otherwise the quadratic polynomial  $x^2 - x$  would have 4 roots in  $\mathbb{F}_4$  which is impossible).

- (2) By definition  $K = \mathbb{F}_8$  and  $[\mathbb{F}_8 : \mathbb{F}_2] = 3$ ,  $\mathbb{F}_8^\times \simeq \mathbb{Z}_7$ : these results follow from the fundamental theorem on finite fields and their extensions.  $\mathbb{F}_4$  is not a sub-field of  $\mathbb{F}_8$  though, since  $[\mathbb{F}_4 : \mathbb{F}_2] = 2 \nmid [\mathbb{F}_8 : \mathbb{F}_2] = 3$ .