

**Cimpa research school on  
 Arithmetic in action:  
 Number Theory and its Applications to Cryptography and Coding Theory  
 Universitas Gadjah Mada  
 Course on Algebraic Number Theory  
 F. Pazuki and V. Talamanca  
 Problem set 1**

**Problem 1.** Let  $F$  be a number field of degree  $n$ .

- a. Show that for  $a \in \mathbb{Q}$  one has
  - $\text{Tr}_F(ax) = a \text{Tr}_F(x)$  for all  $x \in F$ .
  - $\text{Tr}_F(a) = na$ .
  - $N_F(a) = a^n$ .
- b. Prove that the trace map  $\text{Tr}_F : F \rightarrow \mathbb{Q}$  is surjective.
- c. Provide a counterexample for the analogous statement about the norm map  $N_F : F \rightarrow \mathbb{Q}$ .

**Problem 2.** Let  $F = \mathbb{Q}(\sqrt[4]{2})$  and consider  $\alpha = \sqrt{2} = (\sqrt[4]{2})^2 \in F$ .

- a. Compute the characteristic polynomial of  $\alpha$  as element of  $F$ , and compute  $\text{Tr}_F(\alpha)$  and  $N_F(\alpha)$ .
- b. Note that  $\alpha$  belongs to the subfield  $F' = \mathbb{Q}(\sqrt{2})$ . Compute the characteristic polynomial of  $\alpha$  as element of  $F'$ , and compute  $\text{Tr}_{F'}(\alpha)$  and  $N_{F'}(\alpha)$ . Compare with what you found in a.

**Problem 3.** Let  $F \subset K$  be an extension of number fields of degree  $d$ . Show that

$$N_K(x) = N_F(x)^d \quad \text{and} \quad \text{Tr}_K(x) = d \text{Tr}_F(x)$$

for all  $x \in F$ .

**Problem 4.** Let  $F = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ .

- a. Prove that  $F = \mathbb{Q}(\sqrt{3} + \sqrt{5})$ .
- b. Compute  $\Delta(1, \sqrt{3}, \sqrt{5}, \sqrt{15})$  and  $\Delta(1, \sqrt{3}, \sqrt{5}, \sqrt{3} + \sqrt{5})$ .

**Problem 5.** (Vandermonde) Let  $\alpha_1, \dots, \alpha_n$  be elements of a commutative ring  $A$ . Prove the equality

$$\det \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{pmatrix} = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i).$$

**Problem 6.** Let  $f \in \mathbb{Q}[x]$  and suppose that  $f(x) = \prod_{i=1}^n (x - \alpha_i)$ , for  $\alpha_i$  in a splitting field of  $f$ . Define the discriminant of  $f$  as

$$\text{disc}(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

- a. Verify that for quadratic polynomial the discriminant above defined coincide with the usual discriminant.
- b. Suppose that  $F = \mathbb{Q}(\alpha)$  is a number field. Let  $f$  be the minimal polynomial of  $\alpha$ . Show that

$$\Delta(1, \alpha, \dots, \alpha^{n-1}) = \text{disc}(f).$$

**Problem 7.** Let  $F$  be a number field of degree 2 (also called a quadratic number field). Prove that there exists a unique square free integer  $d$ , such that  $F = \mathbb{Q}(\sqrt{d})$ .

**Problem 8.** Let  $F = \mathbb{Q}(\sqrt{d})$ , and  $\alpha = a + b\sqrt{d}$ .

- a. Prove that  $\alpha \in \mathcal{O}_F$  if and only if both  $2a$  and  $a^2 - b^2d$  belong to  $\mathbb{Z}$ .
- b. Prove that if  $\alpha \in \mathcal{O}_F$ , then  $2a$  is even if and only if  $2b$  is even.
- c. Prove that if  $\alpha \in \mathcal{O}_F$ , then  $2a$  and  $2b$  are both even, then  $\mathcal{O}_F = \mathbb{Z}[\sqrt{d}]$ .

- d. Prove that if  $2a$  and  $2b$  are both odd, then  $d \equiv 1 \pmod{4}$ , and  $\mathcal{O}_F = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ .  
 e. Conclude that  $\mathcal{O}_F = \mathbb{Z}[\sqrt{d}]$  if  $d \equiv 2, 3 \pmod{4}$ , while  $\mathcal{O}_F = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$  if  $d \equiv 1 \pmod{4}$ .

**Problem 9.** Let  $F = \mathbb{Q}(\sqrt[3]{20})$ .

- a. Show that  $\mathbb{Z}[\sqrt[3]{20}, \sqrt[3]{50}]$  is contained in  $\mathcal{O}_F$  the ring of integers of  $F$ .  
 b. Let  $c \in \mathbb{Q}$  be such that  $c\sqrt[3]{20} \in \mathcal{O}_F$  or  $c\sqrt[3]{50} \in \mathcal{O}_F$ , show that  $c \in \mathbb{Z}$ .  
 c. Let  $a, b \in \mathbb{Q}$  and suppose  $x = a\sqrt[3]{20} + b\sqrt[3]{50} \in \mathcal{O}_F$ .  
     ◦ Show that  $2a$  and  $5b$  belong to  $\mathbb{Z}$  (Hint  $x\sqrt[3]{20}$  and  $x\sqrt[3]{50}$  belong to  $\mathcal{O}_F$ ).  
     ◦ Show that  $a, b \in \mathbb{Z}$  (Hint:  $x^2$  belongs to  $\mathcal{O}_F$ ).  
 d. Use c. to prove that  $\mathcal{O}_F = \mathbb{Z}[\sqrt[3]{20}, \sqrt[3]{50}]$ .

**Problem 10.** Let  $F = \mathbb{Q}(\sqrt[3]{20})$ .

- a. Show that the discriminant of  $F$  is  $-2700$ .  
 b. Let  $x = a\sqrt[3]{20} + b\sqrt[3]{50}$ , for some integers  $a, b$ . Show that  $\Delta(1, x, x^2) = -2700(2a^3 - 5b^3)^2$ .  
 c. Show that the equation  $2a^3 - 5b^3 = \pm 1$  has no integer solutions (Hint: reduce modulo 7 or 9). Conclude that  $\mathcal{O}_F$  is not of the form  $\mathbb{Z}[\alpha]$ .

**Problem 11.** Let  $d \neq 1$  be a square free integer. Let  $F$  be the quadratic field  $\mathbb{Q}(\sqrt{d})$ . Show that the discriminant of  $F$  is given by

$$\Delta_F = \begin{cases} 4d & \text{if } d \equiv 2, 3 \pmod{4} \\ d & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$