

THE UNIVERSITY OF SYDNEY
FACULTY OF SCIENCE

MATH3962

Rings, Fields and Galois Theory (Advanced)

June, 2007

Time allowed: two hours

Lecturer: R. B. Howlett

No notes or books are to be taken into the examination room.

This paper will be marked out of 120. The marks for each question are shown.

The symbols \mathbb{Z} , \mathbb{Q} , \mathbb{R} and \mathbb{C} denote the rings of integers, rational numbers, real numbers and complex numbers respectively.

1. (i) Let R be a ring and 0_R its zero element. Working directly from the ring axioms, prove that $a0_R = 0_R$ for all $a \in R$. *(6 marks)*
- (ii) Let R and S be integral domains with identity elements 1_R and 1_S respectively. Prove that if $\phi: R \rightarrow S$ is a nonzero homomorphism then $\phi(1_R) = 1_S$. *(7 marks)*
- (iii) Show by means of an example that the result of Part (ii) is not true if R and S are merely assumed to be commutative rings with identity elements. *(7 marks)*

2. Let $i = \sqrt{-1} \in \mathbb{C}$, and let $\mathbb{G} = \{n + mi \mid n, m \in \mathbb{Z}\}$, the ring of all Gaussian integers. For each $\alpha \in \mathbb{C}$ let $|\alpha| \in \mathbb{R}$ be defined in the usual way.
 - (i) Let $\alpha = n + mi$ be an arbitrary nonzero element of \mathbb{G} . Show that for each $\beta \in \mathbb{G}$ there exist $\kappa, \rho \in \mathbb{G}$ with $\beta = \kappa\alpha + \rho$ and $|\rho|^2 \leq \frac{1}{2}|\alpha|^2$. *(7 marks)*
 - (ii) Prove that every ideal in \mathbb{G} is principal. *(7 marks)*
 - (iii) Find an element $\alpha \in \mathbb{G}$ such that $\mathbb{G}/\alpha\mathbb{G}$ is isomorphic to $\mathbb{Z}/29\mathbb{Z}$, and prove this isomorphism. (It is useful to observe that α and $i\alpha$ have coprime imaginary parts.) *(6 marks)*

3. Let $F = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$, the field extension of \mathbb{Q} generated by $\sqrt{2}$ and $\sqrt[3]{5}$.
- (i) Determine $[F : \mathbb{Q}]$, the degree of the extension, and find a basis for F considered as a vector space over \mathbb{Q} . (Any results proved in the lectures or the notes may be used without proof.) (10 marks)
- (ii) Show that if $\alpha \in F$ then the function $\phi_\alpha: F \rightarrow F$ defined by $\phi_\alpha\beta = \alpha\beta$ (for all $\beta \in F$) is a \mathbb{Q} -linear transformation of F . (5 marks)
- (iii) Find a matrix with rational entries that has $\sqrt{2} + \sqrt[3]{5}$ as an eigenvalue. (10 marks)
4. Let F_0 be a field isomorphic to $\mathbb{Z}/p\mathbb{Z}$, where p is a (positive) prime integer, and let F be an extension of F_0 with $[F : F_0] = 3$.
- (i) Show that F has exactly p^3 elements. (7 marks)
- (ii) Show that $F_0[x]$ has p^2 monic polynomials of degree 2, of which $\frac{1}{2}p(p+1)$ are reducible and $\frac{1}{2}p(p-1)$ irreducible. Hence show that there are exactly $\frac{1}{6}p(p-1)(p-2) + p(p-1) + p + p(\frac{1}{2}p(p-1))$ reducible monic polynomials of degree 3. (9 marks)
- (iii) Calculate the total number of monic irreducible polynomials of degree 3 in $F_0[x]$, and prove that they all have exactly three roots in F . (9 marks)
5. Let $f(x)$ be an irreducible cubic polynomial in $\mathbb{Q}[x]$ and let α, β, γ be the roots of $f(x)$ in \mathbb{C} . Let $E \subseteq \mathbb{C}$ be the splitting field for $f(x)$ over \mathbb{Q} .

- (i) Let δ be the determinant of the matrix

$$M = \begin{pmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{pmatrix}.$$

Show, using Galois theory, that $\delta^2 \in \mathbb{Q}$. (7 marks)

- (ii) With δ as in Part (i), show that $\text{Gal}(E : \mathbb{Q})$ (the Galois group of the extension) has order three if $\delta \in \mathbb{Q}$, order six if $\delta \notin \mathbb{Q}$. (8 marks)
- (iii) Suppose now that $f(x) = x^3 - 3x - 1$.

- (a) Find $\alpha + \beta + \gamma$ and $\alpha^2 + \beta^2 + \gamma^2$, and show also that

$$\alpha^3 + \beta^3 + \gamma^3 = 3(\alpha + \beta + \gamma) + 3$$

and

$$\alpha^4 + \beta^4 + \gamma^4 = 3(\alpha^2 + \beta^2 + \gamma^2) + (\alpha + \beta + \gamma). \quad (5 \text{ marks})$$

- (b) With M and δ as in Part (i), calculate MM^T , where M^T is the transpose of M , and hence find δ^2 . (5 marks)
- (c) Show that $\text{Gal}(E : \mathbb{Q})$ has order 3, and hence show that β and γ are contained in the extension of \mathbb{Q} generated by α . (5 marks)