# MTH 617 Algebraic Number Theory

## First Mid Semester Examination

Total marks: 25 | September 8, 2002 | Time: $1 + \epsilon$ hours

---

**1.** Let $A := \{a + b\sqrt{65} \mid a, b \in \mathbb{Z}\}$. For $a + b\sqrt{65} \in A$ (with $a, b \in \mathbb{Z}$) define $\mathrm{N}(a + b\sqrt{65}) := a^2 - 65b^2$.

**(a)** Convince yourself that $A$ is a ring. **(0)**

**(b)** Show that $\mathrm{N}$ is multiplicative, i.e., $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$ for every $\alpha, \beta \in A$. **(1)**

**(c)** Let $\alpha \in A$. Show that $\alpha$ is a unit of $A$, if and only if $\mathrm{N}(\alpha) = \pm 1$. **(2)**

**(d)** Conclude that there are infinitely many solutions in integers of both the Diophantine equations $x^2 - 65y^2 = 1$ and $x^2 - 65y^2 = -1$. **(3)**

**2.** Let $A$ be a ring and $\mathfrak{a}$ an ideal of $A$. Define $\mathfrak{a}[X]$ to be the set of all polynomials with coefficients from $\mathfrak{a}$. Prove the following assertions:

**(a)** $\mathfrak{a}[X]$ is an ideal in $A[X]$. **(1)**

**(b)** If $\mathfrak{p}$ is a prime ideal of $A$, $\mathfrak{p}[X]$ is also a prime ideal of $A[X]$. **(3)**

**(c)** If $\mathfrak{m}$ is a maximal ideal of $A$, $\mathfrak{m}[X]$ is not necessarily a maximal ideal of $A[X]$. **(2)**

**3.** Let $K := \mathbb{Q}(\sqrt{5}) = \{x + y\sqrt{5} \mid x, y \in \mathbb{Q}\}$ and let $\mathfrak{O} := \left\{a + b\left(\frac{1+\sqrt{5}}{2}\right) \mid a, b \in \mathbb{Z}\right\} \subseteq K$.

**(a)** Verify that $\mathfrak{O}$ is a ring. **(1)**

* **(b)** Show that for $\alpha \in K$ the (monic) minimal polynomial $\mathrm{minpoly}_{\alpha,\mathbb{Q}}(X)$ is in $\mathbb{Z}[X]$, if and only if $\alpha \in \mathfrak{O}$. **(3)**

**(c)** Prove that $\mathfrak{O}$ is a free $\mathbb{Z}$-module of rank 2 generated by 1 and $\frac{1+\sqrt{5}}{2}$. **(1)**

**(d)** Do $1$ and $\sqrt{5}$ also constitute a $\mathbb{Z}$-basis of $\mathfrak{O}$? **(1)**

**4.** A field extension $F \subseteq K$ is called *normal*, if every irreducible polynomial in $F[X]$ that has a root in $K$ splits in $K[X]$. For example, we have proved that every finite extension of finite fields is normal.

* **(a)** If $K$ is the splitting field of a non-constant polynomial $f(X) \in F[X]$ over $F$, show that $F \subseteq K$ is a normal extension. (**Hint:** Let $g(X) \in F[X]$ be irreducible and have a root $\alpha \in K$. Let $\beta$ be another root of $g(X)$. Consider the splitting fields of $f$ and $\mu^*(f)$ over $F(\alpha)$ and $F(\beta)$, where $\mu : F(\alpha) \to F(\beta)$ is an isomorphism.) **(4)**

**(b)** If $[K : F] = 2$, show that $F \subseteq K$ is a normal extension. **(1)**

**(c)** Consider the tower $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ of field extensions to conclude that if $F \subseteq K$ and $K \subseteq L$ are normal extensions, then $F \subseteq L$ need not be normal. **(1)**

**5.** Let $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ be a finite extension of finite fields and $\mathrm{Aut}_{\mathbb{F}_q} \mathbb{F}_{q^m}$ the group of $\mathbb{F}_q$-automorphisms of $\mathbb{F}_{q^m}$. Consider the *Frobenius endomorphism* $\sigma : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ that maps $\alpha \mapsto \alpha^q$. Prove the following assertions:

**(a)** $\sigma \in \mathrm{Aut}_{\mathbb{F}_q} \mathbb{F}_{q^m}$. **(2)**

**(b)** The maps $\mathrm{id}_{\mathbb{F}_{q^m}} = \sigma^0, \sigma, \sigma^2, \ldots, \sigma^{m-1}$ are distinct $\mathbb{F}_q$-automorphisms of $\mathbb{F}_{q^m}$, where $\sigma^i$ denotes the $i$-fold composition of $\sigma$ taking $\alpha \mapsto \alpha^{q^i}$. **(1)**

**(c)** Any $\varphi \in \mathrm{Aut}_{\mathbb{F}_q} \mathbb{F}_{q^m}$ satisfies $\varphi = \sigma^i$ for some $i \in \{0, \ldots, m-1\}$. Thus $\mathrm{Aut}_{\mathbb{F}_q} \mathbb{F}_{q^m}$ is a cyclic group of order $m$ generated by $\sigma$. (**Hint:** An $\mathbb{F}_q$-automorphism of $\mathbb{F}_{q^m}$ maps $\alpha \in \mathbb{F}_{q^m}$ to a conjugate (over $\mathbb{F}_q$) of $\alpha$.) **(3)**

---

Instructor: Dr. Abhijit Das, Department of Mathematics, Indian Institute of technology, Kanpur, India