MTH 617 Algebraic Number Theory

Solutions of the exercises appearing in the First Mid Semester Examination

---

1. (a) I am convinced. Are you too?

(b) For $a, b, c, d \in \mathbb{Z}$ one has $\mathrm{N}((a + b\sqrt{65})(c + d\sqrt{65})) = \mathrm{N}((ac + 65bd) + (ad + bc)\sqrt{65}) = (ac + 65bd)^2 - 65(ad + bc)^2 = (a^2c^2 + 65^2b^2d^2 + 130abcd) - (65a^2d^2 + 65b^2c^2 + 130abcd) = (a^2 - 65b^2)(c^2 - 65d^2) = \mathrm{N}(a + b\sqrt{65})\,\mathrm{N}(c + d\sqrt{65})$.

(c) Let $\alpha \in A^*$, i.e., $\alpha\beta = 1$ for some $\beta \in A$. Then $1 = \mathrm{N}(1) = \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$. Since $\mathrm{N}(\alpha)$ and $\mathrm{N}(\beta)$ are integers, one must have $\mathrm{N}(\alpha) = \pm 1$. Conversely, let $\mathrm{N}(a + b\sqrt{65}) = \pm 1$, i.e., $a^2 - 65b^2 = (a + b\sqrt{65})(a - b\sqrt{65}) = \pm 1$, i.e., $a + b\sqrt{65} \in A^*$.

(d) $(x, y) = (8, 1)$ is a solution of $x^2 - 65y^2 = -1$. The element $\alpha := 8 + \sqrt{65} \in A$ is a unit in A, since $\mathrm{N}(\alpha) = -1$. Note that α has infinite multiplicative order (in A^*), for if not, $\alpha^n = 1$ for some $n \in \mathbb{N}$, i.e., α is a root of unity. Since α is real, one must then have $\alpha = \pm 1$, a contradiction. Thus the elements $\alpha, \alpha^2, \alpha^3, \ldots$ are all distinct. Moreover, for every $n \in \mathbb{N}$ one has $\mathrm{N}(\alpha^n) = (\mathrm{N}(\alpha))^n = \begin{cases} 1 & \text{if } n \text{ is even,} \\ -1 & \text{if } n \text{ is odd.} \end{cases}$

(**Remark:** N is called the norm function of A. Later we shall define norms of elements in general number fields. This exercise illustrates how some purely elementary number-theoretic questions can be handled algebraically. Part (d) can be proved using the theory of continued fractions. But that elementary proof is long and boring. Enjoy the elegance of algebra!)

2. (a) Let $f, g \in \mathfrak{a}[X]$ and $h \in A[X]$. Since $\mathfrak{a}$ is an ideal in A, it easily follows that $f(X) \pm g(X)$ and $h(X)f(X)$ are again polynomials with coefficients from $\mathfrak{a}$. Thus $\mathfrak{a}[X]$ is an ideal in $A[X]$.

(b) Let $f(X) := a_mX^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0, g(X) := b_nX^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0 \in A[X]$ and $h(X) := f(X)g(X) = \sum_{k=0}^{m+n} c_kX^k$, where $c_k := \sum_{i+j=k} a_ib_j$. Assume that $f(X) \notin \mathfrak{p}[X]$ and $g(X) \notin \mathfrak{p}[X]$, i.e., some a_i and some b_j are not elements of $\mathfrak{p}$. Let r (resp. s) be the smallest non-negative integer such that $a_r \notin \mathfrak{p}$ (resp. $b_s \notin \mathfrak{p}$). Then $a_0, \ldots, a_{r-1}$ and $b_0, \ldots, b_{s-1}$ are all elements of $\mathfrak{p}$ and therefore $c_{r+s} = a_rb_s + \sum_{\substack{i+j=r+s \\ i<r \text{ or } j<s}} a_ib_j \notin \mathfrak{p}$, since $\mathfrak{p}$ is a prime ideal in A. Thus $h(X) \notin \mathfrak{p}[X]$.

(c) Let $A := \mathbb{Z}$ and $\mathfrak{m} := 2\mathbb{Z}$. Then $\mathfrak{m}[X]$ is the ideal in $A[X]$ generated by (the constant polynomial) 2. But $\mathfrak{m}[X] = \langle 2 \rangle \subsetneqq \langle X, 2 \rangle \subsetneqq A[X]$, i.e., $\mathfrak{m}[X]$ is not maximal in $A[X]$.

3. (a) The only non-trivial ring axiom to verify in this case is that the product $\alpha\beta$ of $\alpha := a + b\left(\frac{1+\sqrt{5}}{2}\right)$ and $\beta := c + d\left(\frac{1+\sqrt{5}}{2}\right)$ in $\mathfrak{O}$ is again in $\mathfrak{O}$ (where $a, b, c, d \in \mathbb{Z}$). But simple calculations demonstrate that $\alpha\beta = (ac + bd) + (ad + bc + bd)\left(\frac{1+\sqrt{5}}{2}\right) \in \mathfrak{O}$.

(b) Let $\gamma := \frac{1+\sqrt{5}}{2}$. Note that $K = \mathbb{Q}(\gamma)$, i.e., $[K : \mathbb{Q}] = 2$, since γ is a root of the irreducible polynomial $X^2 - X - 1 \in \mathbb{Q}[X]$. Thus the minimal polynomial of every $\alpha \in K$ must be of degree 1 or 2.

First let $\alpha := a + b\left(\frac{1+\sqrt{5}}{2}\right) \in \mathfrak{O}$ with $a, b \in \mathbb{Z}$. If $b = 0$, then $\mathrm{minpoly}_{\alpha,\mathbb{Q}}(X) = X - a \in \mathbb{Z}[X]$. On the other hand, if $b \neq 0$, one can easily show that $\mathrm{minpoly}_{\alpha,\mathbb{Q}}(X) = X^2 - (2a + b)X + (a^2 + ab - b^2) \in \mathbb{Z}[X]$. Conversely, let $\alpha := \frac{a+b\gamma}{c} = \frac{2a+b}{2c} + \frac{b}{2c}\sqrt{5} \in K$ (with $a, b \in \mathbb{Z}, c \in \mathbb{N}$) have $f(X) := \mathrm{minpoly}_{\alpha,\mathbb{Q}}(X) \in \mathbb{Z}[X]$. If $\alpha \in \mathbb{Q}$, then $f(X) = X - r$ for some $r \in \mathbb{Z}$. It follows from $f(\alpha) = 0$ that $\alpha = r \in \mathbb{Z} \subseteq \mathfrak{O}$. So assume that $\alpha \in K \setminus \mathbb{Q}$, so that $b \neq 0$ and $f(X) = X^2 - rX + s$ for some $r, s \in \mathbb{Z}$. Since $f(\alpha) = 0$, we have $(2a + b)^2 - 2rc(2a + b) + 5b^2 - 4sc^2 = -2b(2a + b - rc)\sqrt{5}$. Again since $\sqrt{5}$ is irrational and $b \neq 0$, we must have $2a + b - rc = 0$ and $(2a + b)^2 - 2rc(2a + b) + 5b^2 - 4sc^2 = 0$. Combining these equations gives $r^2c^2 - 2rc(rc) + 5b^2 - 4sc^2 = 0$, i.e., $5b^2 = c^2(r^2 - 4s)$. Looking at the prime factorizations of the two sides of the last equation allows us to conclude that $r^2 - 4s = 5t^2$ for some $t \in \mathbb{N}$. Then $\alpha = \frac{r}{2} \pm \frac{t}{2}\sqrt{5} = \frac{r \mp t}{2} \pm t\gamma$. Since $r^2 - 4s = 5t^2$, one has $r^2 \equiv t^2 \pmod 2$, i.e., r and t have the same parity, i.e., $r \mp t$ is even. Thus $\alpha \in \mathfrak{O}$.

(c) It is sufficient to show that 1 and γ are linearly independent over $\mathbb{Z}$. Let $a + b\gamma = 0$ for $a, b \in \mathbb{Z}$. Then $(2a + b) = -b\sqrt{5}$. But then the irrationality of $\sqrt{5}$ implies that $a = b = 0$.

(d) 1 and $\sqrt{5}$ do not form a $\mathbb{Z}$-basis of $\mathfrak{O}$, since $0+\gamma = \frac{1}{2}+\frac{1}{2}\sqrt{5}$ is not a $\mathbb{Z}$-linear combination of 1 and $\sqrt{5}$. Note that the above $\mathbb{Q}$-linear combination of γ is unique, since 1 and $\sqrt{5}$ form a $\mathbb{Q}$-basis of K.

(**Remark:** Note that both $\{1,\sqrt{5}\}$ and $\left\{1,\frac{1+\sqrt{5}}{2}\right\}$ are $\mathbb{Q}$-bases of K. But $\left\{1,\frac{1+\sqrt{5}}{2}\right\}$ is a $\mathbb{Z}$-basis of $\mathfrak{O}$, whereas $\{1,\sqrt{5}\}$ is not. Also note that everything in this exercise remains true, if 5 is replaced by any square-free integer $m \neq 0,1$ congruent to 1 modulo 4.)

4. **(a)** Let $\gamma_1,\ldots,\gamma_d \in K$ be all the roots of f. Then $K = F(\gamma_1,\ldots,\gamma_d)$. Now let $\alpha \in K$ be a root of a non-constant irreducible polynomial $g(X) \in F[X]$. I will show that any root β of $g(X)$ is also in K. We know that there exists a field isomorphism $\mu : F(\alpha) \to F(\beta)$ that fixes all the elements of F (Lemma 1.70). Clearly K is the splitting field of f over $F(\alpha)$. Let K' be the splitting field of $\mu^*(f) = f$ over $F(\beta)$. By Proposition 1.71 the fields K and K' are isomorphic, i.e., $K = F(\alpha)(\gamma_1,\ldots,\gamma_d) \cong F(\beta)(\gamma_1,\ldots,\gamma_d) = K'$. Thus $K \cong F(\gamma_1,\ldots,\gamma_d)(\beta) = K(\beta)$, i.e., $\beta \in K$.

(b) Let $[K:F] = 2$ and $\alpha \in K$ a root of a non-constant monic irreducible polynomial $g(X) \in F[X]$. Then $g(X) = \text{minpoly}_{\alpha,F}(X) \in F[X]$ and hence $\deg g \mid [K:F] = 2$. If $\deg g = 1$, then $g(X) = X - \alpha$ splits over K. If $\deg g = 2$, then $g(X) = (X-\alpha)(X-\beta) = X^2 - (\alpha+\beta)X + \alpha\beta \in F[X] \subseteq K[X]$. Since α and $\alpha+\beta$ are in K, we must then have $\beta \in K$, i.e., $g(X)$ splits over K.

(c) The extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ is not normal, since $X^4 - 2$ has a root (namely, $\sqrt[4]{2}$) in $\mathbb{Q}(\sqrt[4]{2})$, but $\mathbb{Q}(\sqrt[4]{2})$ being a real field does not contain the imaginary roots $\pm \mathrm{i}\sqrt[4]{2}$ of $X^4 - 2$.

(**Remark:** This exercise illustrates that two popular properties enjoyed by finite fields do not necessarily hold for fields of characteristic 0. First, a finite extension $F \subseteq K$ of fields of characteristic 0 is not necessarily normal. Second, for such an extension $F \subseteq K$ the field K need not be the splitting field of some polynomial in $F[X]$.)

5. **(a)** Let α be a generator of the cyclic group $\mathbb{F}_{q^m}^*$. Since $|\mathbb{F}_{q^m}^*| = q^m - 1$ is coprime to q, it follows that $\sigma(\alpha) = \alpha^q$ is also a generator of $\mathbb{F}_{q^m}^*$, i.e., $\sigma|_{\mathbb{F}_{q^m}^*}$ and hence σ are surjective. σ, being a field homomorphism, is injective too. Finally, if $\alpha \in \mathbb{F}_q$, then $\sigma(\alpha) = \alpha^q = \alpha$.

(b) As above let α be a generator of $\mathbb{F}_{q^m}^*$. Then $\sigma^0(\alpha) = \alpha, \sigma^1(\alpha) = \alpha^q, \sigma^2(\alpha) = \alpha^{q^2}, \ldots, \sigma^{m-1}(\alpha) = \alpha^{q^{m-1}}$ are all distinct.

(c) Again let α be a generator of $\mathbb{F}_{q^m}^*$ and let $f(X) \in \mathbb{F}_q[X]$ be the minimal polynomial of α over $\mathbb{F}_q$. Then $\varphi(\alpha)$ is a root of $\varphi^*(f)$. But φ fixes elements of $\mathbb{F}_q$ and therefore $\varphi^*(f) = f$, i.e., $\varphi(\alpha)$ is again a root of f. Since f is irreducible over $\mathbb{F}_q$, we must have (See Corollary 1.81) $\varphi(\alpha) = \alpha^{q^i} = \sigma^i(\alpha)$ for some i, $0 \leqslant i \leqslant m-1$. Now let $\beta \in \mathbb{F}_{q^m}$ be arbitrary. If $\beta = 0$, then $\varphi(\beta) = 0 = \sigma^i(\beta)$. On the other hand, if $\beta \neq 0$, then $\beta = \alpha^j$ for some j (α being a generator of $\mathbb{F}_{q^m}^*$). Then $\varphi(\beta) = \varphi(\alpha^j) = (\varphi(\alpha))^j = (\alpha^{q^i})^j = (\alpha^j)^{q^i} = \beta^{q^i} = \sigma^i(\beta)$. Thus $\varphi = \sigma^i$.