MATEMATISKA INSTITUTIONEN
UPPSALA UNIVERSITET
Examinator: Veronica Crispin Quiñonez

Kortfattade lösningsförslag till tentamen
Algebraiska strukturer 10 hp
2018-01-11 kl 08-13

---

(1) (a) F [maximal is prime] (b) T (c) F [PID is UFD] (d) F [$\{\pm 1\}$] (e) F [unary] (f) T (g) F [$=(21)(23)(25)$] (h) F (i) F [p^k elements] (j) T [dividing an equilateral triangle in the right way gives a right triangle with the other angles α and 2α such that $\alpha = 30°$]

(2) (a) For every $a \in \mathbb{Z}$ we have $\frac{a}{3^n} \in \mathbb{Q}$. Further $\frac{1}{3^n} \cdot 0 = 0 \in \frac{1}{3^n}\mathbb{Z} \neq \emptyset$ and for all $a, b \in \mathbb{Z}$: $\frac{a}{3^n} - \frac{b}{3^n} = \frac{a-b}{3^n} \in \frac{1}{3^n}\mathbb{Z}$. (1 p)

(b) By above $0 \in H$. Further, any two elements in H we can write as $\frac{a}{3^r}\mathbb{Z}, \frac{b}{3^s}$ for some $a, b \in \mathbb{Z}$ and $r, s \in \mathbb{N}$. Then $\frac{a}{3^r} - \frac{b}{3^s} = \frac{3^s a - 3^r b}{3^{rs}} \in \frac{1}{3^{rs}}\mathbb{Z}$. (2 p)

(c) Firstly, as $\frac{a}{3^n} = \frac{3a}{3^{n+1}}$ we have $\frac{1}{3^n}\mathbb{Z} \subset \frac{1}{3^{n+1}}\mathbb{Z} = \langle \frac{1}{3^{n+1}} \rangle$, which is simply generated. For any fixed $N \in \mathbb{N}$ there is always a rational number $\frac{a}{3^{N+1}}$ with a being non-multiple of 3, that does not belong to $\frac{1}{3^N}\mathbb{Z}$. (2 p)

(3) $20 \cdot 18 = 2^3 \cdot 3^2 \cdot 5$. By The fund. thm for fin. gen. ab. grps (0,5 p), we have the following direct products of this order: $C_8 \times C_9 \times C_5$, $C_8 \times C_3 \times C_3 \times C_5$; $C_2 \times C_4 \times C_9 \times C_5$, $C_2 \times C_4 \times C_3 \times C_3 \times C_5$; $C_2 \times C_2 \times C_2 \times C_9 \times C_5$, $C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5$. (4,5 p)

(4) (a) All 2-products of transpositions are in V_4. By straightforward calculations one shows that $\alpha\sigma\alpha^{-1} \in V_4$ for all $\alpha \in S_4$ (considering a random 4-cycle, 3-cycle and transposition) and every $\sigma \in V_4$. (2 p)

(b) - (1 p) (c) $\{(1)\} < \langle (12)(34) \rangle < V_4 < A_4 < S_4$. (2 p)

(5) (a) - (1 p) (b) Since $\mathbb{Z}[i] \subset \mathbb{C}$, any zerodivisor in $\mathbb{Z}[i]$ is a zerodivisor in $\mathbb{C}$, which is impossible as tha latter is a field. (2 p)

(b) In $\mathbb{C}$ we have $(a+bi)^{-1} = \frac{a-bi}{\sqrt{a^2+b^2}}$. For that to be a Gaussian integer we must have $\frac{a}{\sqrt{a^2+b^2}} = n$, $\frac{b}{\sqrt{a^2+b^2}} = m$ for $n, m \in \mathbb{Z}$. After some arithmetics we get $a^2 + b^2 = (n^2 + m^2)(a^2 + b^2)$ so $n^2 + m^2 = 1$, that is, $n = \pm 1$, $m = 0$ or vice versa. More similar arithmetics gives the units $\{\pm 1, \pm i\}$. (2 p)

(6) (a) No, no, yes. (3 p) (b) Assume $\langle x, y \rangle = \langle f(x, y) \rangle$. But by polynomial and degree arguments there is no $f(x, y)$ such that $x = f(x, y) \cdot p(x, y)$ and $y = f(x, y) \cdot q(x, y)$. (1 p) $\langle 4, x \rangle$ is not principle (showed on lectures). (1p)

(7) (a) α is a root of $f = x^4 + 2x^2 + 25 \in \mathbb{Q}[x]$. f has no roots in $\mathbb{Z}$; further, assuming $f = (x^2 + ax + b)(x^2 + cx + d)$ gives to a system of equations in $\mathbb{Z}[x]$:

$$\begin{cases} a + c = 0 \\ b + ac + d = 2 \\ ad + bc = 0 \\ bd = 25 \end{cases}$$

solving which leads to now integer solutions. Thus, f is irreducibleby Gauss′ lemma. (2 p)

(b) $[\mathbb{Q}[\alpha] : \mathbb{Q}] = \deg f = 4$ (2 p)

(b) The set $\{1, \alpha, \alpha^2, \alpha^3\}$ is linearly independent and, hence, is a basis. (2 p)

(8) Let $\omega = e^{\frac{2\pi i}{5}}$. Then $E = \mathbb{Q}[\omega]$ and $q(x) = Irr(\omega : \mathbb{Q}) = \frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1$, which is irreducible as $q(x + 1)$ is irreducible by the Eisenstein's criterion for $p = 5$. (1 p) $\mathbb{Q} \subset E$ is normal (splitting field) and separable (char 0), so it is Galois. $\mathrm{Gal}(E/\mathbb{Q})$ permutes the roots of $q(x)$, and $\phi(\omega) = \omega^2$ generates all the $\mathbb{Q}$-automorphisms: $\phi^2(\omega) = \omega^4$ (the complex conjugation), $\phi^3(\omega) = \omega^3$, $\phi^4(\omega) = \iota$. Since ϕ^2 has order 2, $\mathrm{Gal}(E/\mathbb{Q}) \cong C_2 \times C_2$. (3 p)

The only non-trivial proper subgroup of $\mathrm{Gal}(E/\mathbb{Q})$ is $\langle \phi^2 \rangle$, and its fixed field is the only intermediate field. (1 p) Extra. $\phi^2(a + b\omega + c\omega^2 + c\omega^3)$ is fixed if $b = 0, c = d$ $\big($having in mind that $\omega^4 = -1 - \omega - \omega^2 - \omega^3$ because of $q(x)\big)$. Thus, $Fix_E(\phi^2) = \mathbb{Q}[\omega^2 + \omega^3]$. In fact, $\omega^2 + \omega^3 = 2cos(\frac{4\pi}{5})$ using trigonometry.