Exam Algebraic Structures, Thursday May 7th 2015, 18.30–21.30. (Possible points: 40, including 4 for free.)

(1) Given the ring $R = \mathbb{Z}[\sqrt{-23}]$ and in it the ideal $I = R \cdot 3 + R \cdot (1 - \sqrt{-23})$. Present complete arguments for all assertions.
   (a) [2 points] Is I a principal ideal?
   (b) [2 points] Is I maximal?
   (c) [2 points] Show that $I^2 = (9, 1 + 5\sqrt{-23})$.
   (d) [2 points] Show that $I^3 = (2 + \sqrt{-23})$.
   (e) [2 points] Is $2 + \sqrt{-23} \in R$ irreducible?
   (f) [2 points] Is R Euclidean?

(2) In this exercise n is an integer and $f_n := x^3 + nx^2 + (n+1)x - 1$.
   (a) [2 points] Show for all $n \in \mathbb{Z}$: $f_n \bmod 2 \in \mathbb{F}_2[x]$ is irreducible.
   (b) [2 points] For which $m > 0$ does $f_n \bmod 2$ split completely in $\mathbb{F}_{2^m}[x]$?
   (c) [2 points] Show that for all $n \in \mathbb{Z}$ the polynomial $f_n \in \mathbb{Z}[x]$ is irreducible.
   (d) [2 points] Does $n \in \mathbb{Z}$ exist such that f_n has a multiple zero in $\mathbb{C}$?
   (e) [2 points] Show that for all odd prime numbers p, $n \in \mathbb{Z}$ exists such that $f_n \bmod p \in \mathbb{F}_p[x]$ has a factor of degree 1.
   (f) [2 points] Show that for every $n \in \mathbb{Z}$ it holds that $f_n \in \mathbb{Z}[i][x]$ is irreducible (here $i^2 = -1$).

(3) This exercise discusses the polynomial $x^q - x - 1$ over the finite field $\mathbb{F}_q$.
   (a) [2 points] Show that $x^3 - x - 1 \in \mathbb{F}_3[x]$ is irreducible.
   (b) [2 points] Show that $x^8 - x - 1 \in \mathbb{F}_8[x]$ is reducible. (Hint: first show that if α in some extension field of $\mathbb{F}_8$ satisfies $\alpha \neq 1$ and $\alpha^3 = 1$, then α is a zero of $x^8 - x - 1$.)
   (c) [2 points] Prove for all possible q that $x^q - x - 1$ has no zero in $\mathbb{F}_q$.
   (d) [2 points] Show that if β is a zero of $x^q - x - 1$ in a splitting field over $\mathbb{F}_q$, then $x^q - x - 1 = \prod_{a \in \mathbb{F}_q}(x - \beta - a)$.
   (e) [2 points] From now on let $q = p$ be a prime number, and let K be a splitting field of $x^p - x - 1$ over $\mathbb{F}_p$, and $\varphi : K \to K$ is the automorphism that raises every element of K to the power p. Show that if $\beta \in K$ is a zero of $x^p - x - 1$, then $\varphi(\beta) = \beta + 1$. Use this to prove that φ has order p.
   (f) [2 points] Show that if $\beta \in K$ is a zero of $x^p - x - 1$, then $[\mathbb{F}_p[\beta] : \mathbb{F}_p] = p$. Conclude that $x^p - x - 1 \in \mathbb{F}_p[x]$ is irreducible.