Math 611 Homework 5

Paul Hacking

November 23, 2019

Reading: Dummit and Foote, Sections 8.1, 8.2, 8.3, 9.1, 9.2, 9.3, 9.4, and 9.5.

Justify your answers carefully (complete proofs are expected). All rings are assumed commutative with 1 unless explicitly stated otherwise.

(1) (Optional) Let

$$R = \mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C},$$

the subring of $\mathbb{C}$ generated by $\sqrt{-2}$. Prove that R is a UFD.

(2) Let $\omega = \frac{1}{2}(1 + \sqrt{-3})$, a primitive cube root of unity, and

$$R = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\} \subset \mathbb{C},$$

the subring of $\mathbb{C}$ generated by ω. Prove that R is a UFD. What are the units in R?

(3) (Optional)

(a) Let R be a UFD and $F = \operatorname{ff} R$ its field of fractions. Suppose $f \in R[x]$ is a monic polynomial (a polynomial with leading coefficient equal to 1). Suppose $\alpha \in F$ satisfies $f(\alpha) = 0$. Prove that $\alpha \in R$. (We say a UFD is *integrally closed*.)

(b) Suppose $d \in \mathbb{Z}$ and d is not a square, and let $R = \mathbb{Z}[\sqrt{d}]$. Using part (a) or otherwise, show that R is not a UFD if either (i) there is a prime $p \in \mathbb{N}$ such that p^2 divides d or (ii) $d \equiv 1 \bmod 4$.

(c) Using part (a) or otherwise, show that $\mathbb{C}[x, y]/(y^2 - x^3)$ is not a UFD.

(4) Let $n \in \mathbb{N}$ and $R = \mathbb{Z}[\sqrt{-n}]$. Prove that R is not a UFD for $n \geq 3$.

(5) Let $R = \mathbb{Z}[\sqrt{2}]$. Define

$$\theta \colon R \to R, \quad \theta(a + b\sqrt{2}) = a - b\sqrt{2},$$

and

$$\sigma \colon R \to \mathbb{Z}_{\geq 0}, \quad \sigma(\alpha) = |\alpha \cdot \theta(\alpha)|;$$

explicitly

$$\sigma(a + b\sqrt{2}) = |a^2 - 2b^2|.$$

(a) Show that θ is a ring homomorphism. Deduce that $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$.

(b) Show that $\sigma(\alpha) \neq 0$ for $\alpha \neq 0$.

(c) Show that $\alpha \in R$ is a unit iff $\sigma(\alpha) = 1$.

(d) Find a unit $\alpha \in R$, and use it to prove that there are infinitely many units in R.

(e) Show that R is a UFD.

(6) (Optional) Let F be a field. Prove that there are infinitely many monic irreducible polynomials in $F[x]$.

(7) (Optional) Determine the irreducible polynomials in $\mathbb{Z}/2\mathbb{Z}[x]$ of degree ≤ 4.

(8) For each of the following polynomials, determine its factorization into irreducibles in $\mathbb{Q}[x]$.

(a) $x^3 + 4x + 1$.

(b) $x^4 + 10x^2 + 9$.

(c) $x^6 - 1$.

(d) $x^4 + 3x^3 + 5x^2 + x + 7$.

(e) $x^n + 57$, where $n \in \mathbb{N}$.

(9) Let $f(x) = x^6 + x^4 + x + 3$. Here are the factorizations of the reduction of f modulo p into irreducibles for the first few primes p :

$$\begin{array}{rcll} f(x) & \equiv & (x+1)(x^2+x+1)(x^3+x+1) & \bmod 2 \\ f(x) & \equiv & x(x+2)(x^4+x^3+2x^2+2x+2) & \bmod 3 \\ f(x) & \equiv & (x+3)^2(x^4+4x^3+3x^2+x+2) & \bmod 5 \\ f(x) & \equiv & (x^2+5x+2)(x^4+2x^3+3x^2+2x+5) & \bmod 7 \\ f(x) & \equiv & (x+6)(x^5+5x^4+4x^3+9x^2+x+6) & \bmod 11 \end{array}$$

Prove that f is irreducible in $\mathbb{Q}[x]$.

(10) Let n be a positive integer.

(a) Show that $x^n + y^n - 1$ is irreducible in $\mathbb{C}[x, y]$.

(b) Show that $x^n y + y^n z + z^n x$ is irreducible in $\mathbb{C}[x, y, z]$.

(11) Let $n \in \mathbb{N}$ be a positive integer and $p \in \mathbb{N}$ be a prime. Let

$$f = a_{2n+1}x^{2n+1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

be a polynomial of odd degree $2n + 1$ with integer coefficients. Suppose that p does not divide the leading coefficient a_{2n+1}, p divides $a_{2n}, a_{2n-1}, \ldots, a_{n+1}$, p^2 divides $a_n, a_{n-1}, \ldots, a_0$, and p^3 does not divide a_0. Prove that f is irreducible in $\mathbb{Q}[x]$.

(12) Let $\alpha \in \mathbb{C}$ be a complex number. Consider the ring homomorphism

$$\varphi : \mathbb{Q}[x] \to \mathbb{C}, \quad \varphi(f(x)) = f(\alpha).$$

(a) Show that either $\ker(\varphi) = \{0\}$, in which case we say α is *transcendental*, or $\ker(\varphi) = (m)$ where $m \in \mathbb{Q}[x]$ is a monic irreducible polynomial, in which case we say α is *algebraic* and m is the *minimal polynomial of* α *over* $\mathbb{Q}$.

(b) Show that $\mathbb{Q}[\alpha] := \varphi(\mathbb{Q}[x])$ is a field iff α is algebraic.

(13) (Optional) Let $p \in \mathbb{N}$ be a prime, and $R = \mathbb{Z}[i]$ the ring of Gaussian integers. Show that the ring $R/(p)$ is (i) a field of order p^2 for $p \equiv 3 \bmod 4$, (ii) isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$ for $p \equiv 1 \bmod 4$, and (iii) isomorphic to $(\mathbb{Z}/p\mathbb{Z})[x]/(x^2)$ for $p = 2$.

Hints:

1 Prove that R is a Euclidean domain (similar to the proof for $\mathbb{Z}[i]$ given in class).

2 Similar to Q1.

3 a Write α as a fraction in its lowest terms and clear denominators in the equation $f(\alpha) = 0$. bc Find an element $\alpha \in \operatorname{ff} R \setminus R$ that satisfies a monic polynomial equation with integer coefficients.

4 Use the norm $N(\alpha) = \alpha\bar{\alpha}$ to show that 2 is irreducible, and divide into cases n even or odd.

5 e Prove that R is a Euclidean domain with size function σ.

6 Adapt the usual argument for prime integers.

7 Use the polynomial version of the Sieve of Eratosthenes. Note that if F is a field and $f \in F[x]$ is reducible then f has an irreducible factor g such that $\deg g \leq \deg f/2$.

8 a If $f \in \mathbb{Q}[x]$ has $\deg f \leq 3$, and f has no roots in $\mathbb{Q}$, then F is irreducible in $\mathbb{Q}[x]$ (why?). Also if $f = a_n x^n + \cdots + a_0$ and $\alpha = a/b \in \mathbb{Q}$ is a rational root of f expressed in its lowest terms, then b divides a_n and a divides a_0. d Consider reduction modulo a prime. e What is Eisenstein's criterion?

9 What are the possible degrees of irreducible factors of f?

10 Use the generalized Eisenstein criterion.

11 Similar to the proof of the Eisentein criterion, suppose f is reducible in $\mathbb{Q}[x]$, then using the Gauss Lemma $f = gh$, some $g, h \in \mathbb{Z}[x]$, $0 < \deg g < \deg h$ (note $\deg g \neq \deg h$ because $\deg f$ is odd). Reduce modulo p, and consider the coefficient of x^m in f, where $m = \deg g$. Deduce p^3 divides a_0, a contradiction.

12 What are the prime ideals in a PID?

13 $\mathbb{Z}[i] \simeq \mathbb{Z}[x]/(x^2+1)$, so $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}/p\mathbb{Z}[x]/(x^2+1)$. What are the solutions of $x^2 + 1 \equiv 0 \bmod p$?