Math 611 Homework 7

Paul Hacking

November 19, 2015

All rings are assumed to be commutative with 1.

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

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

(3) 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 $n \in \mathbb{N}$.

(4) 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 $\mathbb{C}[x, y, z]$.

(5) 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 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 $\mathbb{Q}[x]$.

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

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

(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.

(7) Let $p \in \mathbb{N}$ be a prime, and $R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ 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 $p = 2$.

(8) Let F be a field. Let $R = F[x]$ and consider the R-module $M = R/(x^n)$. Interpret M as an F-vector space $M = V$ together with a linear transformation $T\colon V \to V$ given by $T(v) = x \cdot v$ (scalar multiplication of $v \in V = M$ by $x \in R$). Write down a basis of V as an F-vector space and compute the matrix A of T with respect to this basis.

(9) Let R be a ring and $M = R^n$ a free R-module. For each of the following statements, give a proof or a counterexample.

(a) Any linearly independent set in M can be extended to a basis of M.

(b) Any spanning set of M contains a basis of M.

(c) Let $\varphi\colon M \to M$, $\varphi(\mathbf{x}) = A\mathbf{x}$ be an R-module homomorphism.

i. If φ is injective, then it is an isomorphism.

ii. If φ is surjective, then it is an isomorphism.

(10) Let R be a ring and $f \in R[x]$ a polynomial of degree $n > 0$.

(a) Show that if the leading coefficient of f is a unit then the quotient ring $R[x]/(f)$ is a free R-module of rank n.

(b) Show that $\mathbb{Z}[x]/(2x - 1)$ is not a free $\mathbb{Z}$-module.

(11) Let R be a integral domain and F its field of fractions. Let $A \in R^{m \times n}$ be an $m \times n$ matrix with entries in R, defining a homomorphism of free R-modules

$$\varphi\colon R^n \to R^m, \quad \mathbf{x} \mapsto A\mathbf{x}.$$

Let

$$\varphi_F\colon F^n \to F^m, \quad \mathbf{x} \mapsto A\mathbf{x}$$

be the associated linear transformation of F-vector spaces. Show that φ is injective iff φ_F is injective. (In particular, if φ is injective then $n \leq m$.)

(12) Let R be a ring and $A \in R^{m \times n}$ an $m \times n$ matrix with entries in R. Show that the following conditions are equivalent

(a) The R-module homomorphism $\varphi\colon R^n \to R^m$ given by $\varphi(\mathbf{x}) = A\mathbf{x}$ is surjective.

(b) There exists a matrix $B \in R^{n \times m}$ such that $AB = I_m$ (the $m \times m$ identity matrix).

(c) First, we have $n \geq m$. Second, let J be the ideal of R generated by the $m \times m$ minors of A (the determinants of the matrices formed by a choice of m columns of A). Then $J = R$.

(13) Let $R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ be the ring of Gaussian integers.

(a) Show that an R-module M can be interpreted as an abelian group $M = A$ together with a homomorphism $\varphi\colon A \to A$ such that $\varphi(\varphi(x)) = -x$ for all $x \in A$.

(b) For which prime numbers p can the abelian group $A = \mathbb{Z}/p\mathbb{Z}$ be made into an R-module? What about $A = (\mathbb{Z}/p\mathbb{Z})^2$?

(14) Let F be a field and $R = F[x, y]$.

(a) Show that an R-module M can be interpreted as an F-vector space $M = V$ together with two linear transformations $S\colon V \to V$ and $T\colon V \to V$ such that $S \circ T = T \circ S$.

(b) Using part (a) or otherwise, give an example of two 5×5 matrices A and B such that $AB = BA$ and

$$A^i B^j = 0 \iff i \geq 2 \text{ or } j \geq 3 \text{ or } (i \geq 1 \text{ and } j \geq 2).$$

Hints:

(1) Adapt Euclid's argument that there are infinitely many prime integers.

(2) To find all irreducibles of degree $\leq N$: First list all nonconstant polynomials with $\mathbb{Z}/2\mathbb{Z}$ coefficients of degree $\leq N$ in order of increasing degree. (It is best to use a systematic total order, e.g., so that the coefficients of the nth polynomial in the list are the digits of the integer $n+1$ written in base 2.) Now use the sieve method: at each step the first polynomial in the list is irreducible. Remove nontrivial multiples of that polynomial from the list. Repeat. Note: (i) $(x-\alpha)$ divides f iff $f(\alpha)=0$ and (ii) once we have removed multiples of irreducibles of degree $\leq d$ the remaining polynomials of degree $\leq 2d+1$ are necessarily irreducible (why?). For $\mathbb{Z}/p\mathbb{Z}$, the same procedure applied to monic polynomials gives all irreducibles up to units (a unit in $F[x]$ is a nonzero constant).

(3) (a) For F a field and $f \in F[x]$ a polynomial of degree ≤ 3, f is irreducible in $F[x]$ iff f does not have a root in F (why?). Also, if R is a UFD, and $\alpha = a/b \in F = \operatorname{ff} R$ is a root of $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ expressed in its lowest terms ($\gcd(a,b)=1$), then a divides a_0 and b divides a_n (why?). (d) Reduce mod 2 and use Q2. (e) What is Eisenstein's criterion?

(4) Both polynomials can be shown to be irreducible using the generalized Eisenstein criterion for the polynomial ring $R[x]$, $R = \mathbb{C}[y]$ or $\mathbb{C}[y,z]$, and a prime ideal $P = (f) \subset R$ for some irreducible element $f \in R$ together with the Gauss Lemma. (In more detail, the Eisenstein criterion shows the polynomial is irreducible in $F[x]$ where $F = \operatorname{ff} R$ is the fraction field of R; now by the Gauss Lemma it is irreducible in $R[x]$ iff it is primitive.)

(5) Follow the strategy of the proof of the Eisenstein criterion: Suppose f is reducible in $\mathbb{Q}[x]$, then by the Gauss Lemma $f = gh$ in $\mathbb{Z}[x]$ where $\deg(g), \deg(h) > 0$. Reduce mod p and deduce properties of the coefficents of g and h. Now, since $\deg(f)$ is odd we have $\deg(g) \neq \deg(h)$, say $m = \deg(g) < \deg(h)$. Consider the coefficient of x^m in f. Derive a contradiction by showing p^3 divides a_0.

(6) (b) Use HW6Q1b.

(7) We have $\mathbb{Z}[i] \simeq \mathbb{Z}[x]/(x^2+1)$, so

$$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[x]/(p, x^2+1) \simeq (\mathbb{Z}/p\mathbb{Z})[x]/(x^2+1).$$

(Compare the proof of the classification of primes in $\mathbb{Z}[i]$ given in class.) Now use the fact that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic to describe the factorization of x^2+1 modulo p.

(9) (a), (b), and (c)(i) are false for $R = \mathbb{Z}$ and $n = 1$. (c)(ii) If φ is surjective then there exists $B \in R^{n \times n}$ such that $AB = I_n$ (why?). Deduce that $\det A$ is a unit and so A is invertible.

(10) (a) What is the division algorithm in $R[x]$? (b) Compare HW6Q5a.

(12) (b) $\Rightarrow$ (c): The columns of AB are linear combinations of the columns of A. Deduce using the multilinearity of the determinant that $\det(AB)$ is a linear combination of the determinants of the matrices formed by a choice of m columns of A. (c) $\Rightarrow$ (b): Let $I \subset \{1, \ldots, n\}$ be a subset of size m and A_I be the $m \times m$ matrix formed by the columns of A labelled by I. We have $(\det A_I) I_m = A_I \cdot \operatorname{adj} A_I$ for each I. Now use the assumption on the minors $\det A_I$ to construct a $n \times m$ matrix B such that $AB = I_m$.

(14) (b) Consider $M = F[x,y]/I$ for some ideal $I \subset F[x,y]$.