1 Homework 4.

- 1. Prove that the following polynomials are irreducible.
 - (a) $f(x) := x^{p-1} + x^{p-2} + \cdots + 1$ where p is a prime number.
 - (b) $g(x,y) := x^{p-1} + q_2(y)x^{p-2} + \cdots + q_{p-1}(y)$ in $\mathbb{Q}[x,y]$ where p is prime and $q_i(y)$'s are in $\mathbb{Q}[y]$ such that $q_i(1) = 1$ for all i.
 - (c) $k(x,y) := x^n y$ in F[x,y] where F is a field.
 - (d) $p(x,y) := x^2 + y^2 2$ in F[x,y] where F is a field and its characteristic is not 2.
 - (e) $q(x) := x^4 + 12x^3 9x + 6$ in $\mathbb{Q}[i][x]$.
 - (f) Suppose n is a positive odd integer. Prove that

$$r(x) := (x-1)(x-2)\cdots(x-n) + 1$$

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

(**Hint**. (a) Argue that f(x) is irreducible precisely when $\overline{f}(x) := f(x+1)$ is irreducible. Notice that

$$\overline{f}(x) = \frac{(x+1)^p - 1}{x}.$$

Use Eisenstein's criterion and show that $\overline{f}(x)$ is irreducible in $\mathbb{Q}[x]$.

- (b) Notice that $\mathbb{Q}[y]$ is a UFD and $\langle y-1 \rangle$ is a maximal ideal of $\mathbb{Q}[y]$. Argue that if g(x,y) is not irreducible in $(\mathbb{Q}[y])[x]$, then there are monic polynomials $g_1, g_2 \in (\mathbb{Q}[y])[x]$ that are of x-degree less than p-1 and $g = g_1g_2$. Look at both side modulo $\langle y-1 \rangle$; this is the same as saying that you are evaluating both sides at y=1. Argue why you get a contradiction.
- (c) Multiply by p!, and use a criterion.
- (d) y is irreducible in F[y] and F[y] is a UFD.
- (e) $y^2 2$ is square-free in F[y] and F[y] is a UFD.
- (f) Think about irreducible factors of the coefficients and Eisenstein's criterion. Notice that $\mathbb{Z}[i]$ is a UFD.
- (g) Suppose the contrary. Argue that there exist $r_1, r_2 \in \mathbb{Z}[x]$ of positive degree such that $r(x) = r_1(x)r_2(x)$. Consider r(j) for integer j in [1, n], and think about $r_1(x)^2 1$ and $r_2(x)^2 1$.)

2. Suppose p is a prime in \mathbb{Z} , $a \in \mathbb{Z}$, and $p \nmid a$. Prove that $x^{p^n} - x + a$ does not have a zero in \mathbb{Q} .

(**Hint.** Use the rational root criterion and Fermat'a little theorem.)

3. In this problem, you will need basic properties of the determinant function that I summarize here. For $[a_{ij}] \in M_n(A)$, let

$$\det[a_{ij}] := \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^n a_{i\sigma(i)},$$

where S_n is the symmetric group and $\operatorname{sgn}: S_n \to \{\pm 1\}$ is the sign function. The (ℓ, k) -minor of $x := [a_{ij}]$ is the determinant of the (n-1)-by-(n-1) matrix $x(\ell, k)$ obtained after removing the ℓ -th row and the k-th column of x. Let

$$adj(x) := [(-1)^{i+j} \det x(j,i)] \in M_n(A);$$

this is called the adjugate of A. Here are the main properties of det and adj.

- (a) det is multi-linear with respect to the columns and rows.
- (b) $\det(I) = 1$.
- (c) If x has two identical columns or rows, then $\det x = 0$.
- (d) For all $x, y \in M_n(A)$, det(xy) = det(x) det(y).
- (e) adj(x)x = x adj(x) = det(x)I.

For every A-module homomorphism $\phi: A^n \to A^n$, similar to linear maps, we can associate a matrix $x_{\phi} \in M_n(A)$; the *i*-th column of x_{ϕ} is given by the vector $\phi(e_i)$, where e_i has 1 at the *i*-th component and 0 at the other components. In this setting, ϕ is an A-module isomorphism if and only if x_{ϕ} is a unit in $M_n(A)$.

- (a) Prove that x is a unit in $M_n(A)$ if and only if $\det x \in A^{\times}$.
- (b) Suppose $\phi:A^n\to A^n$ is an A-module. Prove that the following statements are equivalent.
 - i. ϕ is surjective.

ii. For all maximal ideals \mathfrak{m} of A, the induced A/\mathfrak{m} -linear map

$$\overline{\phi}: (A/\mathfrak{m})^n \to (A/\mathfrak{m})^n, \quad \overline{\phi}(x+\mathfrak{m}^n) := \phi(x) + \mathfrak{m}^n$$

is a well-defined bijection.

iii. ϕ is bijective.

(**Hint**. For linear maps from a vector space to itself, we know that surjectivity implies injectivity. So the first part implies the second part. To show the third part, suppose $\det(x_{\phi})$ is not a unit, and deduce that there exists a maximal ideal such that x_{ϕ} modulo \mathfrak{m} is not invertible.)

4. Suppose A is a unital commutative ring and $\phi: A^n \to A^m$ is a surjective A-module homomorphism. Prove that $n \geq m$.

(**Hint**. Think about
$$\overline{\phi}: (A/\mathfrak{m})^n \to (A/\mathfrak{m})^m$$
.)

- 5. An A-module M is called Noetherian if the following equivalent statements hold.
 - (a) Every chain $\{N_i\}_{i\in I}$ of submodules of M has a maximum.
 - (b) Every non-empty family of submodules of M has a maximal element.
 - (c) The ascending chain condition holds in M; that means if

$$N_1 \subseteq N_2 \subseteq \cdots$$

are submodules of M, then there exists i_0 such that

$$N_{i_0} = N_{i_0+1} = \cdots$$
.

(d) All the submodules of M are finitely generated.

Use a similar argument as in the case for rings and show that the above statements are equivalent; you do not need to submit this as part of your HW assignment. Notice that a ring A is Noetherian if and only if it is a Noetherian A-module.

(a) Suppose N is a submodule of M. Prove that M is Noetherian if and only if M/N and N are Noetherian.

- (b) Suppose A is a Noetherian ring and M is a finitely generated A-module. Prove that M is Noetherian.
- 6. Suppose A is a unital commutative ring and $\phi: A^n \to A^m$ is an injective A-module homomorphism.
 - (a) Suppose A is a Noetherian ring. Prove that $n \leq m$.
 - (b) Prove that $n \leq m$ even if A is not Noetherian.

(**Hint**. For the first part, suppose to the contrary that n > m and write A^n as $A^m \oplus A^{n-m}$. This way, you can view the image of ϕ as a submodule of A^n and

$$\phi(A^n) \oplus A^{n-m} \subseteq A^n.$$

Because ϕ is injective, we obtain that

$$\phi^2(A^n) \oplus \phi(A^{n-m}) \oplus A^{n-m} \subseteq A^n$$
.

Repeating this argument, for every positive integer k, we obtain the following (internal) direct sum:

$$\phi^k(A^n) \oplus \phi^{k-1}(A^{n-m}) \oplus \cdots \oplus \phi(A^{n-m}) \oplus A^{n-m} \subseteq A^n.$$

Hence,

$$A^{n-m} \subsetneq A^{n-m} \oplus \phi(A^{n-m}) \subsetneq A^{n-m} \oplus \phi(A^{n-m}) \oplus \phi^2(A^{n-m}) \subsetneq \cdots$$

which is a contradiction.

For the second part, let $x_{\phi} \in \mathcal{M}_{m,n}(A)$ be the matrix associated with ϕ . Let A_0 be the subring of A which is generated by 1 and entries of x_{ϕ} . Notice that since ϕ is given by matrix multiplication by x_{ϕ} , its restriction to A_0^n gives us an A_0 -module homomorphism from A_0^n to A_0^m . Because ϕ is injective, so is its restriction to A_0^n . Argue why A_0 is Noetherian, and deduce that $n \leq m$.

Remark. During lecture, we used field of fractions and gave a much easier proof when A is an integral domain.

7. Suppose A is a unital commutative ring and M is a finitely generated A-module. Let

$$d(M) := minimum number of generators of M,$$

and

rank(M) := maximum number of linearly independent elements of M.

Prove that $rank(M) \leq d(M)$.

(**Hint**. Suppose d(M) = n and rank(M) = m. Then there exist a surjective A-module homomorphism

$$\phi: A^n \to M$$

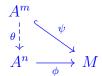
and an injective A-module homomorphism

$$\psi: A^m \to M$$
.

Suppose $\{e_i\}_{i=1}^m$ is the standard A-base of A^m . Deduce that there exist $v_i \in A^n$ such that

$$\phi(v_i) = \psi(e_i)$$

for all i. Let $\theta:A^m\to A^n$ be the A-module homomorphism given by $\theta(e_i)=v_i$ for all i. Then the following diagram commutes.



Deduce that θ is injective.)

- 8. Suppose A is a unital commutative ring and M is a finitely generated A-module. Suppose $d(M) = \operatorname{rank}(M) = n$.
 - (a) Suppose A is Noetherian. Prove that $M \simeq A^n$.
 - (b) Prove that $M \simeq A^n$ even if A is not Noetherian.

(**Hint**. Similar to the previous problem, get a commutative diagram

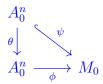


where ψ is injective and ϕ is surjective, and obtain that θ is injective. Use injectivity of ψ and deduce that the following is an internal direct sum

$$\theta(A^n) \oplus \ker \phi \subseteq A^n$$
.

Use an argument similar to problem 5(a) to deal with the Noetherian case; show that if ker $\phi \neq 0$, we get a contradiction.

To show the general case, again suppose to the contrary that there exists $\mathbf{x} := (x_1, \dots, x_n) \in \ker \phi \setminus \{0\}$. Let $x_{\theta} \in \mathrm{M}_n(A)$ be the matrix associated with θ . Let A_0 be the subring of A which is generated by 1, x_i 's, and entries of x_{θ} . Let $M_0 := \phi(A_0^n)$. Argue why we have the following commutative diagram



and θ and ψ are injective, and $\mathbf{x} \in \ker \phi$. Discuss why A_0 is Noetherian, and obtain a contradiction.)

Remark. There is a much easier argument when A is an integral domain. Think about that case.