HOMEWORK 9, DUE THU APR 8TH

All solutions should be with proofs, you may quote from the book or from previous home works

(1) Let p be a prime number.

(a) Show that the polynomial $x^n - p$ is irreducible in $\mathbb{Q}[x]$.

Solution. Notice that $x^n - p \in \mathbb{Z}$ and is primitive, since it is monic. Just apply Eisenstein criterion with the prime p. $\square$

(b) Show that $f(x) = \frac{x^p-1}{x-1} = 1 + x + \cdots + x^{p-1}$ is irreducible over the rationals. (Hint: Put $x = y + 1$ and use Eisenstein.)

Solution. Using the hint, $\frac{x^p-1}{x-1} = \frac{(y+1)^p-1}{y}$. If we expand by binomial theorem,

$$(y+1)^p = y^p + \binom{p}{1}y^{p-1} + \binom{p}{2}y^{p-2} + \cdots + \binom{p}{p-1}y + 1.$$

Thus, we get,

$$f(x) = y^{p-1} + \binom{p}{1}y^{p-2} + \binom{p}{2}y^{p-3} + \cdots + \binom{p}{p-1}.$$

It is an easy exercise to show that, since p is a prime, all the coefficients of y^k with $k < p-1$ are divisible by p and since the constant coefficient is $\binom{p}{p-1} = p$, it is not divisible by p^2. So, Eisenstein applies.

$\square$

(c) Write $x^6 - 1$ as a product of irreducible polynomials in $\mathbb{Q}[x]$.

Proof.

$$\begin{aligned} x^6 - 1 &= (x^3-1)(x^3+1) \\ &= (x-1)(x^2+x+1)(x+1)(x^2-x+1) \end{aligned}$$

$x-1, x+1$ are irreducible (linear polynomials are always irreducible), x^2+x+1 is irreducible by using part (b) with $p=3$ and x^2-x+1 is irreducible, since if you substitute $-x$ for x in this, we just get x^2+x+1. So, the above is the required product. $\square$

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

(a) Show that the only units in A are ± 1.

Solution. If $x \in A$ is a unit, we have $xy = 1$ for some $y \in A$. Taking complex conjugates (which are still in A), we see that $\overline{x}$, the complex conjugate of x is also a unit and thus so is $x\overline{x}$. If $x = a + b\sqrt{-5}$, $x\overline{x} = a^2 + 5b^2 \in \mathbb{Z}$ and a unit, so must be ± 1. The only solutions are $a = \pm 1, b = 0$. $\square$

(b) Show that $3, 2+\sqrt{-5}$ and $2-\sqrt{-5}$ are irreducible in A.

Solution. The proof is similar to the previous step.
Write $3 = xy$ with $x, y \in A$ and we wish to show that one of them is a unit. By taking complex conjugates and multiplying, we get $9 = x\overline{x}y\overline{y}$ and if $x = a + b\sqrt{-5}, y = c + d\sqrt{-5}$, this gives $9 = (a^2+5b^2)(c^2+5d^2)$. If one of these is 9, the other is one and then that would be a unit etc. So,we may assume $a^2 + 5b^2 = 3$. If $b \neq 0$, the left hand side is at least 5 , so $b = 0$ and then we have $a^2 = 3$ which is absurd.
Similarly, write $2+\sqrt{-5} = xy$ and as before, we get $9 = (a^2+5b^2)(c^2+5d^2)$ which will again say one of x, y is a unit. $2-\sqrt{-5}$ case is identical. $\square$

(c) Prove that A is not a PID, using $3^2 = (2+\sqrt{-5})(2-\sqrt{-5})$.

Solution. This follows immediately from the previous part, since in a PID, irreducibility is same as prime. $\square$

(3) Let $A = \mathbb{C}[x,y]/I$ where I is the principal ideal generated by $y^2 - x^3 - x$. We also have an inclusion $B = \mathbb{C}[x] \subset A$ as a subring.

(a) Show that $y^2 - x^3 - x$ is irreducible in $\mathbb{C}[x,y]$ and so, A is an integral domain.

Solution. Treat $p = y^2 - x^3 - x \in B[y]$ as a polynomial in y over B. Since $\deg_y p = 2$, any factor of p must have degree $0, 1$ or 2 in y. If it has a factor of degree zero, then this factor is an element of B and so we must have $q(x)|p$. If $q(x)$ is not a unit, then $\deg_x q > 0$ and so it has a root, say $a \in \mathbb{C}$. Since $p = p(x,y) = q(x)R(x,y)$, we get $p(a,y) = 0$. But, $p(a,y) = y^2 - a^3 - a \neq 0$. So, p has a linear factor and since it is monic, immediate that this factor must be monic. In other words, we should have $p(x,y) = (y - q(x))(y - r(x))$ for $q, r \in B$.

$$(y-q)(y-r) = y^2 - (q+r)y + qr.$$

So, $q + r = 0$ and then $q^2 = x^3 + x$. So, any prime factor of $x^3 + x$ (in B) must occur with multiplicity 2. But $x^3 + x = x(x+i)(x-i)$, has three irreducible factors with multiplicity one. This proves p is irreducible. □

(b) Show that all maximal ideals of B are of the form $(x - a)B$ for some $a \in \mathbb{C}$. (Hint: Fundamental Theorem of Algebra).

Solution. This is just the hint. Maximal ideals of a PID are generated by prime (=irreducible) elements. If $p(x) \in B$ and $\deg p = 0$, then p is a constant (so a unit if non-zero). If $\deg p = 1$, then they are irreducible and any linearl polynomial up to unit is just of the form $x - a$, $a \in \mathbb{C}$. If $\deg p > 1$, let a be a root (by FTA) then division algorithm gives $p(x) = (x-a)q(x)$ and $\deg q > 0$, so p is not irreducible. □

(c) Show that if $M \subset A$ is a maximal ideal of A, then $M \cap B$ is a maximal ideal of B.

Solution. With no assumptions on the rings, we first check that $M \cap B$ is a prime ideal. If $\alpha\beta \in M \cap B$ where $\alpha, \beta \in B$, since M is maximal and hence prime, one of them must be in M and then it is also in $M \cap B$.

We have an inclusion $K = B/M \cap A \subset B/M = L$. Since M is maximal, L is a field. We wish to show that K is a field. Let y denote the image of y in L, by abuse of notation. Then, by division algorithm in A, one easily checks that any element of L can be written uniquely as

$a + by$ with $a, b \in K$ and of course, we have $y^2 = t \in K$, where t is the image of $x^3 + x$ in K. Let $0 \neq u \in K$. Since L is a field, u has an inverse in L, say, $a + by$ with $a, b \in K$. Then, $ua + uby = 1$. This says $ua = 1, ub = 0$, by our uniqueness of such expressions. Thus, $ua = 1$ which means u has an inverse in K. □

(4) Let A be a PID.

(a) Let $R = K_1 \times K_2 \times \cdots \times K_n$, where K_is are fields, with the usual product ring structure. Let $a_1, \ldots, a_m \in R$ such that the ideal generated by these is the whole ring R. Show that we can find $q_2, q_3, \ldots, q_m \in R$ such that $a_1 + q_2a_2 + q_3a_3 + \cdots + q_ma_m$ is a unit in R.

Solution. Write $a_1 = (u_1, \ldots, u_m)$ where $u_i \in K_i$. If all $u_i \neq 0$, then a_1 is unit and we can take $q_i = 0$ for all i. So assume some of them are zero and reordering the fields, we may assume $u_i \neq 0$ for $i \leq r$ and $u_i = 0$ for $i > r$. Since a_is generate the whole ring, there must be some $a_i, i > 1$ such that if we write $a_i = (v_1, \ldots, v_m)$, then $v_{r+1} \neq 0$. Again, we may assume $i = 2$. Assume $v_s \neq 0$ for $r < s \leq r'$. Then take $q_2 = (0, 0, \ldots, 1, \ldots 1)$ where the first r are zeroes. Then, q_2a_2 has zeroes in the first r places and non-zero entries between r and r'. So, when we take $a_1 + q_2a_2$, it has non-zero entries from 1 to r'. If $r' \neq m$, can assume that a_3 has a non-zero entry in the r'th place and continue. □

(b) Let $a_1, \ldots, a_m \in A$ be such that $\gcd(a_1, \ldots, a_m) = 1$. Also assume that $m \geq 3$. Then show that we can find

$$p_2, \ldots, p_m, q_3, \ldots, q_m \in A$$

such that,

$$\gcd(a_1 + p_2a_2 + \cdots + p_ma_m,\ a_2 + q_3a_3 + \cdots + q_ma_m) = 1.$$

Solution. If $a_1 \neq 0$, choose $p_i = 0$ for all i. If not choose p_i so that $a_1 + p_2a_2 + \cdots + p_ma_m \neq 0$, which can be done since at least one of the $a_i \neq 0$. So, now onwards, let us assume that $a_1 \neq 0$. If a_1 is a unit, we may choose $q_i = 0$, so assume not. Let $x_1, \ldots, x_n$ be all the primes dividing a_1.

We look at $R = A/\prod x_i A = K_1 \times \cdots \times K_n$ where $K_i = A/p_i A$, by Chinese remainder theorem. Notice that K_is are fields. We call the images of $a_i \in R$ still a_i and since $a_1 = 0 \in R$, we see that $a_2, \ldots, a_m$ generate R, since the ideal generated by $a_1, \ldots, a_m$ in A is all of A. So, by the previous part, we can find $q_3, \ldots, q_m \in R$ so that $a_2 + q_3 a_3 + \cdots + q_m a_m$ is a unit in R. Since $\pi : A \to R$ is onto, we may lift q_is to A and call them still q_i. Then, we see that $\pi(a_2 + q_3 a_3 + \cdots + q_m a_m)$ is a unit in R. This means, none of the x_i divides $a_2 + q_3 a_3 + \cdots + q_m a_m$ and this just means $\gcd(a_1, a_2 + q_3 a_3 + \cdots + q_m a_m) = 1$. □

(c) Let $a_1, \ldots, a_m \in A$ with $\gcd(a_1, \ldots, a_m) = 1$. Show that we can find an invertible matrix U of size m so that,

$$(a_1, \ldots, a_m)U = (1, 0, \ldots, 0).$$

(Do this for $m \leq 3$, which has all the necessary ideas for full credit.)

Solution. If $m = 1$, then a_1 is a unit and we can take $U = [a_1^{-1}]$. If $m = 2$, since the ideal generated by a_1, a_2 is A, we have an equation $1 = a_1 b_1 + a_2 b_2$ for some $b_1, b_2 \in A$. Then, take U to be,

$$U = \begin{bmatrix} b_1 & -a_2 \\ b_2 & a_1 \end{bmatrix}.$$

So, now assume that $m \geq 3$. We assume $m = 3$ for notational simplicity and contains the basic ideas. By part (b) we can find p_2, p_3, q_3 so that $b_1 = a_1 + p_2 a_2 + p_3 a_3$ and $b_2 = a_2 + q_3 a_3$ have gcd 1. Let,

$$A = \begin{bmatrix} 1 & 0 & 0 \\ p_2 & 1 & 0 \\ p_3 & q_3 & 1 \end{bmatrix}.$$

Then, A is lower triangular with 1s on the diagonal, so has determinant one and in particular, invertible. Note that $(a_1, a_2, a_3)A = (b_1, b_2, a_3)$.
Since $\gcd(b_1, b_2) = 1$, we have $c_1, c_2 \in A$ such that $c_1 b_1 + c_2 b_2 = 1$. Now let

$$B = \begin{bmatrix} c_1 & -b_2 & 0 \\ c_2 & b_1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Then, $\det B = 1$ and $(b_1, b_2, a_3)B = (1, 0, a_3)$. Finally, let

$$C = \begin{bmatrix} 1 & 0 & -a_3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Again, $\det C = 1$ and $(1, 0, a_3)C = (1, 0, 0)$. So, take $U = ABC$. □

(d) Using the above and imitating the proof we did in class, show that any torsion free finitely generated module over A is free.

Solution. Let M be a torsion free finitely generated module over A. Pick $e_1, \dots, e_n \in M$ a set of generators where n is minimum. We wish to show that these are linearly independent. If not, we have a relation $a_1e_1 + \cdots + a_ne_n = 0$ with at least one $0 \neq a_i \in A$. So, we can consider $d = \gcd(a_1, \dots, a_n)$. As we did in class, we may assume $d = 1$, since otherwise, write $a_i = db_i$ and then $d(b_1e_1 + \cdots b_ne_n) = 0$. Since M is torsion free, we get $b_1e_1 + \cdots + b_ne_n = 0$ and $\gcd(b_1, \dots, b_n) = 1$.
So, we may assume $\gcd(a_1, \dots, a_n) = 1$. Now, by part (c), we have an invertible $n \times n$ matrix U such that $(a_1, \dots, a_n)U = (1, 0, \dots, 0)$. Write

$$U^{-1} \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix} = \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}.$$

Then, it is clear that w_is generate M since U is invertible. Also, we have

$$[a_1, \dots, a_n] \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix} = 0,$$

which we can rewrite as,

$$[a_1, \dots, a_n]UU^{-1} \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix} = 0$$

which says,

$$[1, 0, \dots, 0] \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} = 0.$$

This just says $w_1 = 0$, so M is generated by $w_2, \dots, w_n$, contrary to our choice of n. $\square$