Answersheet 10 - Yiwei Yang 2018533218

1.

Prop 103: Let $\underset{N}{\sim}$ be a Euuclidian function on A. Define N(a)=$min\{\underset{N}{\sim}(ba) \mid b \in A\backslash\{0\}\}$. Then N is a Euclidian Funclion.

Proof: Euclidean norm $\underset{N}{\sim}$ be an Euclidean domain.

1. Then,

$$N(1) = \min\{\underset{N}{\sim}(x) : x \in A, x \neq 0\} \tag{1}$$

2. For $b \in A\backslash\{0\}$ we have

$$b \text{ is a unit } \Longleftrightarrow \underset{N}{\sim}(b) = \underset{N}{\sim}(1) . \tag{2}$$

Then N is a Euclidian Function.

Proof. (1) follows from the second property of $\underset{N}{\sim}$ as follows:

$$\forall a \in D, a \neq 0 \quad \underset{N}{\sim}(1) \leq \underset{N}{\sim}(1a) = \underset{N}{\sim}(a) \tag{3}$$

To prove (2) suppose $b \in \underset{N}{\sim}$ is a unit. Then,

$$\underset{N}{\sim}(1) \leq \underset{N}{\sim}(u) \leq \underset{N}{\sim}\left(bb^{-1}\right) = \underset{N}{\sim}(1). \quad So \quad \underset{N}{\sim}(b) = \underset{N}{\sim}(1) \tag{4}$$

Conversely, suppose $\underset{N}{\sim}(1) = \underset{N}{\sim}(b)$. Se divide ! by u, we have $1 = bq + r$ for some $q, r \in D \quad \ni \quad r = 0$ or $\underset{N}{\sim}(r) < \underset{N}{\sim}(u)$. Since $\underset{N}{\sim}(u) = \underset{N}{\sim}(1)$ is minimum, $r = 0$. So, $1 = bq$. So, b is a unit. The proof is complete.

2.

a.

Suppos e A is a UFD with the field F, Then a non-constant polynomial p_1 in $A[x]$ is irreducible iff it's irreducible in $F[x]$ and the gcd of the coefficient of p_1 is 1.

Proof: First note that the gcd of the coefficients of p_1 is 1 since, otherwise, we can factor out some element $c \in A$ from the coefficients of p_1 to write $p_1 = cp_1'$, contradicting the irreducibility of p_1. Next, suppose $p_1 = p_2p_3$ for some non-constant polynomials p_2, p_3 in $F[x_1, \ldots, x_n]$. Then, for some $d \in A$, the polynomial dp_2 has coefficients in A and so, by factoring out the gcd q of the coefficients, we write $dp_2 = qp_2'$. Do the same for p_3 and we can write $p_1 = cp_2'p_3'$ for some $c \in F$. Now, let $c = a/b$ for some $a, b \in A$. Then $bp_1 = ap_2'p_3'$. From this, using the proposition, we get:
$(b) \supset \gcd(\operatorname{cont}(bp_1)) = (a)$.
That is, b divides a. Thus, $c \in R$ and then the factorization $p_1 = cp_2'p_3'$ constitutes a contradiction to the irreducibility of p_1.

For the other side. If p_1 is irreducible over F, then either it's irreducible over A or it contains a constant polynomial as a factor.

b.

Suppose A is a UFD with the field F, $p_1p_2 \in \mathbb{Q}(A)[X]\backslash\{0\}$. Then $cont(p_1p_2) = cont(p_1)cont(p_2)$.

Proof: Clearly, $\operatorname{cont}(p_1p_2) \subset \operatorname{cont}(p_1)\operatorname{cont}(p_2)$. If $\mathfrak{p}$ is a prime ideal containing $\operatorname{cont}(p_1p_2)$, then $p_1p_2 \equiv 0$ modulo $\mathfrak{p}$. Since $A/\mathfrak{p}\,[x_1, \ldots, x_n]$ is a polynomial ring over an integral domain and thus is an integral domain, this implies either $p_1 \equiv 0$ or $p_2 \equiv 0$ (mod $\mathfrak{p}$). Hence, either $\operatorname{cont}(p_1)$ or $\operatorname{cont}(p_2)$ is contained in $\mathfrak{p}$. Since $\sqrt{\operatorname{cont}(p_1p_2)}$ is the intersection of all prime ideals that contain $\operatorname{cont}(p_1p_2)$ and the choice of $\mathfrak{p}$ was arbitrary, $\operatorname{cont}(p_1)\operatorname{cont}(p_2) \subset \sqrt{\operatorname{cont}(p_1p_2)}$
We now prove the "moreover" part. Factoring out the gcd's from the coefficients, we can write $p_1 = ap_1'$ and $p_2 = bp_2'$ where the gcds of the coefficients of p_1', p_2' are both 1 . Clearly, it is enough to prove the assertion when p_1, p_2 are replaced by p_1', p_2'; thus, we assume the gcd's of the coefficients of p_1, p_2 are both 1 .

We have that if $\operatorname{gcd}(a, b) = \operatorname{gcd}(a, c) = 1$, then $\operatorname{gcd}(a, bc) = 1$
(The proof of the lemma is not trivial but is by elementary algebra.) We argue by induction on the sum of the numbers of the terms in f, g; that is, we assume the proposition has been established for any pair of polynomials with one less total number of the terms. Let (c) $= \operatorname{gcd}(\operatorname{cont}(p_1p_2))$; i.e., c is the gcd of the coefficients of p_1p_2. Assume $(c) \neq (1)$; otherwise, we are done. Let p_1', p_2' denote the highest-degree terms of p_1, p_2 in terms of lexicographical monomial ordering. Then $p_1'p_2'$ is precisely the leading term of p_1p_2 and so c divides the (unique) coefficient of $p_1'p_2'$ (since it divides all the coefficients of p_1p_2). Now, if c does not have a common factor with the (unique) coefficient of p_1' and does not have a common factor with that of p_2', then, by the above lemma, $\operatorname{gcd}(c, \operatorname{cont}(p_1'p_2')) = (1)$. But c divides the coefficient of $p_1'p_2'$; so this is a contradiction. Thus, either c has a common factor with the coefficient of p_1' or does with that of p_2'; say, the former is the case. Let $(d) = \operatorname{gcd}(c, \operatorname{cont}(p_1'))$. Since d divides the coefficients of $p_1p_2 - p_1'p_2 = (p_1 - p_1')\,p_2$, by inductive hypothesis,
$(d) \supset \operatorname{gcd}(\operatorname{cont}((p_1 - p_1')\,p_2')) = \operatorname{gcd}(\operatorname{cont}(p_1 - p_1'))\operatorname{gcd}(\operatorname{cont}(p_2)) = \operatorname{gcd}(\operatorname{cont}(p_1 - p_1'))$.
Since (d) contains $\operatorname{cont}(p_1')$, it contains $\operatorname{cont}(p_1)$; i.e., $(d) = (1)$, a contradiction.

If $\operatorname{gcd}(\operatorname{cont}(p_1p_2)) = (1)$, then there is nothing to prove. So, assume otherwise; then there is a non-unit element dividing the coefficients of p_1p_2. Factorizing that element into a product of prime elements, we can take that element to be a prime element π. Now, we have:

$$(\pi) = \sqrt{(\pi)} \supset \sqrt{\operatorname{cont}(p_1p_2)} \supset \operatorname{cont}(p_1)\operatorname{cont}(p_2) \tag{5}$$

Thus, either (π) contains $\operatorname{cont}(p_1)$ or $\operatorname{cont}(p_2)$; contradicting the gcd's of the coefficients of p_1, p_2 are both 1. $\square$

3.

Eclidean Algorithm :gcd(a,b)=gcd(b,a mod b)

gcd($X^6+3X^5+7X^4+12X^3+15X^2+9X+9$,$X^4+6X^3+13X^2+12X+3$)=gcd(
$X^4+6X^3+13X^2+12X+3$, $-3X^5-6X^4+12X^2+9X+9$) = gcd(
$-3X^5-6X^4+12X^2+9X+9$,$12X^4+51X^3+48X^2+18X+9$) = gcd(
$12X^4+51X^3+48X^2+18X+9$,$6.75X^3+24X^2+13.5X+11.25$) = gcd(
$6.75X^3+24X^2+13.5X+11.25$,$\frac{25}{3}X^3+24X^2-6X-11$) =$X^2+3X+3$

4.

Basic theorem on symmetric polynomials: For a symmetric polynomial F over any domain $f \in F\left(x_1, x_2, \cdots, x_n\right)$, there exists a polynomial $g\left(x_1, x_2, \cdots, x_n\right) \in F\left[x_1, x_2, \ldots, x_n\right]$ such that $f=g\left(\sigma_1, \sigma_2, \cdots, \sigma_n\right)$, that is, can be tabulated by the basic symmetric polynomial polynomial.

$$P(x_1,x_2,x_3) = x_1^2 + x_1^2 x_2 + x_1 x_2 x_3$$

$$Q = \sum_{\sigma \in S_3} \sigma(P)$$

$$x_1(x_1 + x_1 x_2 + x_2 x_3) = x_1\big(\sigma_2(x_1 x_2 x_3) - x_1 x_3 + x_1\big)$$

$$= \sigma_1(x_1)\big(\sigma_2(x_1 x_2 x_3) - \sigma_2(x_1 x_3) + \sigma(x_1)\big)$$

$$\sigma_1 = x_1 + x_2 + x_3$$

$$\sigma_2 = x_1 x_2 + x_3 x_1 + x_2 x_3$$

$$\sigma_3 = x_1 x_2 x_3$$

$$x_1^2 + x_1^2 x_2 + x_1 x_2 x_3$$

$$x_1 x_2 x_3 + x_1^2 + x_2^2 + x_3^2 = \underline{\sigma_1^2 - 2\sigma_2 + \sigma_3}$$

$$x_1^2 x_2 + x_1 x_2^2 + x_2^2 x_3 + x_2 x_3^2 + x_3^2 x_1 + x_3 x_1^2 = \sigma_1 \sigma_2 - 3\sigma_3$$

$$P(x_1 x_2 x_3) + P(x_2 x_3 x_1) + P(x_3 x_1 x_2)$$

$$= \sigma_1^2 - 2\sigma_2 \cancel{+3\sigma_3} + \sigma_1 \sigma_2 \cancel{-3\sigma_3} = \sigma_1^2 - 2\sigma_2 + \sigma_1 \sigma_2$$

$$\Rightarrow \tilde{Q} = \frac{\sigma_1^2 - 2\sigma_2 + \sigma_1 \sigma_2}{3}$$