

Problem Set #2

Due monday 16 September in Class

We recall the following important results good to know:

Let R be a GCD ring, and $f(X) \in R[X]$. Then the **content of f** , $\text{cont}(f(X))$ is the greatest common divisor of the coefficients of $f(X)$.

Lemma 1: If $\text{cont}(F(X)) = \text{cont}(G(X)) = 1$, $F(X), G(X) \in R[X]$, then

$$\text{cont}(F(X)G(X)) = 1.$$

More generally, for $f(X), g(X) \in R[X]$, $\text{cont}(f(X)g(X)) = \text{cont}(f(X))\text{cont}(g(X))$.

Proof of Lemma 1: Suppose irreducible $p \in R$ divides all coefficients of $F(X)G(X)$. Then $F(X)G(X) = 0$ in $(R/p)[X]$, which is an integral domain. Thus p either divides all coefficients of $F(X)$ or p divides all coefficients of $G(X)$, since one of $F(X), G(X)$ must be 0 in $(R/p)[X]$. But this contradicts the assumption $\text{cont}(F) = \text{cont}(G) = 1$. In the general case, write $f = dF$, $g = d'G$, where $\text{cont}(F) = \text{cont}(G) = 1$. Then $fg = dd'FG$, so, by the first part of the Lemma, $\text{cont}(f(X)g(X)) = \text{cont}(f(X))\text{cont}(g(X))$.

Lemma 2 (Gauss): Let K be the field of fractions of R . If $P(X) \in R[X]$ factors in $K[X]$ then $P(X)$ factors in $R[X]$ with factors of the same degrees as the $K[X]$ factors. In particular if $P(X) \in R[X]$ is irreducible if and only if $P(X)$ is also irreducible in $K[X]$.

Proof of Lemma 2: Every element of $K[X]$ can be written $A(X)/a$, where $A(X) \in R[X]$ and $a \in R$. Suppose in $K[X]$, we have $P(X) = (A(X)/a)(B(X)/b)$, with $a, b \in R$ and $A(X), B(X) \in R[X]$. Then $abP(X) = A(X)B(X) \in R[X]$. Consider an irreducible factor p of ab in R . Then $A(X)B(X) = 0$ in $(R/p)[X]$. Thus p either divides all coefficients of $A(X)$ or p divides all coefficients of $B(X)$. We can then cancel a factor p in the $R[X]$ equation $abP(X) = A(X)B(X)$, without leaving $R[X]$. By induction on the number of prime factors of ab in R , conclude $P(X) = A'(X)B'(X) \in R[X]$, where $\deg(A'(X)) = \deg(A(X))$ and $\deg(B(X)) = \deg(B'(X))$.

Theorem 1: R is a UFD then R is a UFD. In Particular, by induction $R[X_1, \dots, X_n]$.

Proof of Theorem 1: First, suppose $f(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$, for

$a_j \in R$. Then define the content of $f(X)$ to be $\text{cont}(f(X)) = \gcd(a_0, \dots, a_n) = d$ in R . (So $\text{cont}(f(X))$ is well-defined up to a unit factor in R .)

(Existence) If $p \in R$ is irreducible then p is also irreducible in $R[X]$. if $f(X) \in R[X]$, write $f(X) = dF(X)$, where $d = \text{cont}(f(X))$. Then $\text{cont}(F(X)) = 1$. We can certainly factor d into a product of irreducibles in R . Either $F(X)$ is irreducible in $R[X]$ or it factors properly as a product of lower degree polynomials (since $\text{cont}(F(X)) = 1$). All the factors will also have content 1 (since a divisor of any factor would divide F .) We can only lower degree of factors finitely often, so we get a factorization of $F(X)$, and hence $f(X)$, as a product of irreducibles in $R[X]$.

(Uniqueness) It suffices to prove each irreducible element of $R[X]$ generates a prime ideal in $R[X]$. For irreducibles $p \in R$ this is clear $R[X]/pR[X] = (R/p)[X]$, which is an integral domain.

Now we finish the proof of Theorem 1 by showing $(P(X)) \subset R[X]$ is a prime ideal if $P(X)$ is irreducible in $R[X]$. Certainly $\text{cont}(P(X)) = 1$ and by the Gauss Lemma $P(X)$ is irreducible in $K[X]$. Suppose $P(X)Q(X) = F(X)G(X) \in R[X] \subset K[X]$. Since $K[X]$ is a PID, we know $P(X)$ divides $F(X)$ or $G(X)$ in $K[X]$. Say in $K[X]$ we have $F(X) = P(X)(S(X)/s)$ with $S(X) \in R[X]$, $s \in R$. Then in $R[X]$ we have $P(X)S(X) = sF(X)$. Then s divides $\text{cont}(P(X)S(X)) = \text{cont}(S(X))$ by Lemma 1. So $S(X)/s$ is in $R[X]$ and $F(X)$ is in the ideal $(P(X)) \subset R[X]$.

Exercise 3 p 15 [N]

In the polynomial ring $A = \mathbb{Q}[X, Y]$, consider the principal ideal $\mathfrak{p} = (X^2 - Y^3)$. Show that \mathfrak{p} is a prime ideal, but A/\mathfrak{p} is not integrally closed.

Solution:

We give different approaches to prove that \mathfrak{p} is a prime ideal:

1. To prove that the polynomial $f(X) = X^2 - Y^3$ is irreducible in $\mathbb{Q}[X, Y]$, it suffices to prove that it is irreducible in $\mathbb{Q}(Y)[X]$. this is clear because being a polynomial of degree 2, it has no root in $\mathbb{Q}(Y)$.
2. We can also prove that we have an isomorphism

$$\mathbb{Q}[X, Y]/(X^2 - Y^3) \simeq \mathbb{Q}[t^2, t^3]$$

and conclude, since $\mathbb{Q}[T^2, T^3]$ being a integral domain implies $(X^2 - Y^3)$ will be a prime ideal.

For this, consider the morphism:

$$\begin{aligned} \phi : \mathbb{Q}[X, Y] &\rightarrow \mathbb{Q}[T^2, T^3] \\ X &\mapsto T^3 \\ Y &\mapsto T^2 \end{aligned}$$

It is clearly a surjective morphism and $(X^2 - Y^3) \subseteq \ker(\phi)$.

Take an element $f(X, Y) \in \text{Ker}(\phi)$, i.e. as a polynomial in variable X and

coefficients coming from $k[Y]$. If you divide $f(X, Y)$ by $(X^2 - Y^3)$, we will get

$$f(X, Y) = g(X, Y)(X^3 - Y^2) + r(X, Y)$$

where $r(X, Y) \in k[Y][X]$ and degree of $r(X, Y)$ is less than two. But then $f(T^3, T^2) = 0$ implies $r(T^3, T^2) = 0$. But if $r(X, Y)$ is not zero, $r(T^3, T^2)$ cannot be zero because $r(X, Y)$ is a polynomial of degree less than two in variable X with coefficients in $K[Y]$. So that $r(T^3, T^2) = 0$ and $f(X, Y) \in \ker(\phi)$.

Note that we could also have just argued by contradiction, supposing that $X^2 - Y^3$ can be factorized and it will be the factorization in $K(X)[Y]$ and argue on the degree and the form of the possible polynomials.

As a consequence it is an integral domain but not integrally closed $t = \bar{x}/\bar{y}$ is in the fraction field and integral (satisfies $z^2 - t^2 = 0$ in $\mathbb{C}[t^2, t^3]$) but not in $\mathbb{C}[t]$

Exercise 4 p 15 [N]

Let D be a square free integer $\neq 0, 1$ and d the discriminant of the quadratic number field $K = \mathbb{Q}[\sqrt{D}]$. Show that

$$\begin{aligned} d = D \text{ and } \{1, (1 + \sqrt{D})/2\} \text{ is an integral basis of } K & \text{ if } D \equiv 1 \pmod{4} \\ d = 4D \text{ and } \{1, \sqrt{D}\} \text{ is an integral basis of } K & \text{ if } D \equiv 2 \text{ or } 3 \pmod{4} \end{aligned}$$

and that $\{1, (d + \sqrt{d})/2\}$ is an integral basis of K in both cases.

Solution:

Let $\alpha \in K$, $\alpha = \frac{a+b\sqrt{D}}{c}$ with $\gcd(a, b, c) = 1$. Claim that $\alpha \in \mathcal{O}_K$ if and only if

$$\left(t - \frac{a + b\sqrt{d}}{c}\right) \in \mathbb{Z}[t]$$

So if and only if

$$1. \quad \frac{2a}{c} \in \mathbb{Z}, \text{ and}$$

$$2. \quad \frac{a^2 - b^2D}{c^2} \in \mathbb{Z}$$

Let $q = \gcd(a, c)$. From (2), $q^2 | a^2 - b^2D$. But $q^2 | a^2$ and D is square free, so $q | b$. But $\gcd(a, b, c) = 1$ so $q = 1$. From (1), then $c = 1$ or 2 . If $c = 1$ then $\alpha \in \mathcal{O}_K$, anyway.

If $c = 2$ then $a^2 - b^2d \equiv 0 \pmod{4}$, by (2). But a is odd as $q = 1$ and so b must be odd too, whence $a^2 \equiv b^2 \equiv 1 \pmod{4}$. Hence, $1 - d \equiv 0 \pmod{4}$.

$$\text{If } D \equiv 1 \pmod{4} \text{ then } d = \left(\det \begin{pmatrix} 1 & 1 \\ (1 + \sqrt{D})/2 & (1 - \sqrt{D})/2 \end{pmatrix} \right)^2 = D$$

$$\text{If } D \equiv 2 \text{ or } 3 \pmod{4} \text{ then } d = \left(\det \begin{pmatrix} 1 & 1 \\ \sqrt{D} & -\sqrt{D} \end{pmatrix} \right)^2 = 4D$$

Then,

$$\begin{aligned} \text{If } D \equiv 1 \pmod{4} \text{ then } (d + \sqrt{d})/2 &= (D + \sqrt{D})/2 \in \mathcal{O}_K \\ \text{If } D \equiv 2 \text{ or } 3 \pmod{4} \text{ then } (d + \sqrt{d})/2 &= 2D + \sqrt{D} \in \mathcal{O}_K \end{aligned}$$

So that, in both cases, $\{1, (d + \sqrt{d})/2\}$ is an integral basis of K .

Exercise 5 p 15 [N]

Show that $\{1, {}^3\sqrt{2}, {}^3\sqrt{2}^2\}$ is an integral basis of $\mathbb{Q}({}^3\sqrt{2})$.

Solution:

Let $K = \mathbb{Q}({}^3\sqrt{2})$. We can calculate $d = \text{disc}(1, {}^3\sqrt{2}, {}^3\sqrt{2}^2)$ using the formula for $\theta = {}^3\sqrt{2}$,

$$\text{disc}(1, \theta, \theta^2) = ((\theta_1 - \theta_2)(\theta_1 - \theta_3)(\theta_2 - \theta_3))^2$$

where $\theta_1 = \theta$, $\theta_2 = e^{\frac{2\pi i}{3}}\theta$, $\theta_3 = e^{\frac{4\pi i}{3}}\theta$, the image of θ by the 3 \mathbb{Q} -embedding $\sigma_1 = \text{Id}$, $\sigma_2 : \theta \mapsto e^{\frac{2\pi i}{3}}\theta$ and $\sigma_3 : \theta \mapsto e^{\frac{4\pi i}{3}}\theta$. Then

$$d = 4 \left(1 - e^{\frac{2\pi i}{3}}\right)^2 \left(e^{\frac{2\pi i}{3}} - e^{\frac{4\pi i}{3}}\right)^2 \left(1 - e^{\frac{4\pi i}{3}}\right)^2 = 108$$

Hence we know that

$$d = \left[O_K : \mathbb{Z} + \mathbb{Z}^3\sqrt{2} + \mathbb{Z}^3\sqrt{4}\right]^2 \text{disc}(O_K) = 108 = 2^2 3^3.$$

The possible values for $i = [O_K : \mathbb{Z} + \mathbb{Z}^3\sqrt{2} + \mathbb{Z}^3\sqrt{4}]$ are the numbers whose squares divide 108, namely 1, 2, 3, and 6. In particular, in each cases, $i|6$. So that

$$iO_K \subseteq \mathbb{Z} + \mathbb{Z}^3\sqrt{2} + \mathbb{Z}^3\sqrt{4}$$

So that if $\alpha = a + b^3\sqrt{2} + c^3\sqrt{4}$ ($a, b, c \in \mathbb{Q}$) is integral over \mathbb{Z} , then the coefficients a , b , and c must have denominator dividing 6 (when the fractions are reduced). Moreover, a product of the denominators must also divide 6. Consider the minimal polynomial of α

$$f(x) = \prod_{i=1}^3 (x - \sigma_i(\alpha)) = x^3 - 3ax^2 + (3a^2 - 6bc)x + (-a^3 - 2b^3 + 6abc - 4c^3).$$

The coefficients of $f(x)$ must be in \mathbb{Z} . The element a cannot have a 2, 3, or 6 in its denominator because otherwise the coefficients of x^2 and x in $f(x)$ would not be integers, as a consequence a is an integer. Similarly, b and c must be integers so that the coefficient of x and the constant term will be integers. Therefore, $[O_K : \mathbb{Z} + \mathbb{Z}^3\sqrt{2} + \mathbb{Z}^3\sqrt{4}] = 1$, and we have equality $O_K = \mathbb{Z} + \mathbb{Z}^3\sqrt{2} + \mathbb{Z}^3\sqrt{4}$.