Class Group, Algebraic Group, and Dedekind Domain Homework

Padmavathi Srinivasan

Due: Thursday, Mar 28th, 11:59 P.M.

Recall the Dedekind domain S from the previous homework defined as follows. Let $F = \mathbb{C}(x)$, let $p(y) = y^2 - x(x-5)(x+5) \in F[y]$ and let $E = F[y]/(p(y))$. Let $R = \mathbb{C}[x]$ $S = R[y]/(p(y))$. Any point $(a,b) \in \mathbb{C}^2$ that lies on the curve $y^2 = x(x-5)(x+5)$ gives rise to a maximal ideal $\wp_{a,b} = (x-a, y-b)$ of S. This procedure in fact gives rise to all maximal ideals of S (see HW2 solutions for a proof).

1. (a) Show that the ideals $\wp_1 = (x,y), \wp_2 = (x-5,y), \wp_3 = (x+5,y)$ give non-trivial 2-torsion elements in the class group of S.

   (b) Compute the prime factorization of the principal ideal (y) in the ring S, and write down the corresponding relation that you obtain in $\mathrm{Cl}(S)$.

   (c) Show that $[\wp_{a,b}]^{-1} = [\wp_{a,-b}]$ in $\mathrm{Cl}(S)$. (Inversion in the class group corresponds to the geometric operation of reflection about the x-axis.)

   (d) Sketch the $\mathbb{R}$-points on the curve $y^2 = x(x-5)(x+5)$. Let L be a line that intersects the curve $y^2 = x(x-5)(x+5)$ in three distinct points P_1, P_2 and P_3. Let $\wp_1, \wp_2$ and $\wp_3$ be the corresponding maximal ideals of S. Show that $[\wp_1] + [\wp_2] + [\wp_3] = 0$ in $\mathrm{Cl}(S)$. Can you now geometrically describe $[\wp_1] + [\wp_2]$ in $\mathrm{Cl}(S)$ in terms of the corresponding points on the curve? [1]

   (e) (Optional challenge problem) Show that the ideal $\wp = (x+4, y-6)$ gives rise to an element of infinite order in the class group of S. [2]

2. Let $R = \mathbb{C}[x]$ and $F = \mathbb{C}(x)$. Show that $R[y]$ is an integrally closed domain that is not of height 1. Show that $S = R[y]/(y^2 - x^3)$ is an integral domain that has height 1 but is not integrally closed. What is the integral closure of S in its fraction field $F[y]/(y^2 - x^3)$? [3]

3. (a) Show that a Dedekind ring R with only finitely many prime ideals is a PID. (Hint: Assume the contrary, and let $\{\wp_1, \wp_2, \ldots, \wp_r\}$ be the set of prime ideals of the Dedekind ring. To find a generator for $\wp_1$, use the Chinese Remainder Theorem to lift a suitable element of $R/\wp_1^2 \times R/\wp_2 \times \ldots \times R/\wp_r$ that is guaranteed to be divisible by $\wp_1$ exactly once, and not divisible by $\wp_i$ for $i \neq 1$.)

   (b) Show that every non-zero ideal I in a Dedekind ring can be generated by two elements. (Let $I = \prod \mathfrak{p}_i^{a_i}$ and let $\alpha \in I \setminus \{0\}$. Let $(\alpha) = \prod \mathfrak{p}_i^{b_i} \prod \mathfrak{q}_j^{c_j}$. Let α be one of your generators and for the second generator, lift a suitable element of $\prod R/\mathfrak{p}_i^{a_i+1} \times \prod R/\mathfrak{q}_j^{c_j}$.)

[1] The set of points on the curve inherits a group structure from the corresponding operations on $\mathrm{Cl}(S)$. The identity element of the group corresponds to the missing limit point on the curve that is far out at infinity. Can you geometrically describe the doubling operation in the group?

[2] The point $x = -4, y = 6$ on the plane curve $y^2 = x(x-5)(x+5)$ is an example of a non-torsion point on an elliptic curve. The proof that I know that this point is non-torsion uses some non-trivial facts from Algebraic geometry. I don't know an elementary proof only using facts that you have learnt in this class – Let me know if you find one! You should be able to prove this after a first course on rational points on elliptic curves from say Silverman's book. One proof ultimately shows that the number of digits needed to describe the numerator and denominator of the point nP grows with n – magic word is "height".

[3] In dimension 1 (i.e. when the ring has height 1), the ring being integrally closed is equivalent to the underlying geometric object (the set of maximal ideals) being nonsingular. The plane curve $y^2 = x^3$ has a singularity at $x = y = 0$.

Class Group, Algebraic Group, and Dedekind Domain Homework

Caitlin Beecham

1. (a) Well, $p_1^2 = (x^2, xy, y^2) = (x^2, xy, x(x-5)(x+5)) = (x^2, xy, x^3 - 25x)$. Then, $x^2 \in p_1^2$ implies that $x^3 \in p_1^2$. Then, $x^3 - 25x - x^3 = -25x \in p_1^2$ so that $x \in p_1^2$ which implies that $(x) \subseteq p_1^2$. Finally, note that $p_1^2 = (x^2, xy, x(x-5)(x+5)) \subseteq (x)$ since x divides each generator of p_1^2. Thus, we have shown $p_1^2 = (x)$ a principal ideal which means that $p_1^2 \in e_{Cl(S)}$ so that $o(\overline{p_1}) = 2$ in the class group (where $\overline{p_1}$ is the equivalence class of p_1 in Cl(S)).

   Now, $p_2^2 = ((x-5)y, y^2, (x-5)^2) = ((x-5)y, (x-5)x(x+5), (x-5)^2) = (xy-5y, x^3-25x, x^2-10x+25)$. Then, $x^2-10x+25 \in p_2^2$ implies that $x^3-10x^2+25x \in p_2^2$. Then, $x^3-10x^2+25x-(x^3-25x) = -10x^2+50x \in p_2^2$ so that $-x^2+5x \in p_2^2$ which implies that $x^2-10x+25-x^2+5x = -5x+25 \in p_2^2$ so that $10x-50 \in p_2^2$. Then, one obtains $x^2-10x+25+10x-50 = x^2-25 \in p_2^2$. Finally, one obtains $x^2-10x+25-x^2+25 = -10x+50 \in p_2^2$ so that $x-5 \in p_2^2$. So, $(x-5) \subseteq p_2^2$. Also, note $p_2^2 \subseteq (x-5)$ since $(x-5)$ divides each generator of p_2^2. So, $p_2^2 = (x-5)$ a principal ideal means that $o(\overline{p_2}) = 2$ in the class group (where $\overline{p_2}$ is the equivalence class of p_2 in Cl(S)).

   Finally, $p_3^2 = ((x+5)^2, (x+5)y, y^2) = (x+5)^2, (x+5)y, (x+5)(x-5)x) = (x^2+10x+25, xy+5y, x^3-25x)$. Then, note that $x^2+10x+25 \in p_3^2$ implies that $x^3+10x^2+25x \in p_3^2$ so that $x^3+10x^2+25x-(x^3-25x) = 10x^2+50x \in p_3^2$. Then, $x^2+10x+25-(x^2+5x) = 5x+25 \in p_3^2$, which implies that $x+5 \in p_3^2$. So, that gives $(x+5) \subseteq p_3^2$. Furthermore $p_3^2 \subseteq (x+5)$ since $(x+5)$ divides each generator of p_3^2 which means that each generator belongs to $(x+5)$. So, $p_3^2 = (x+5)$ a principal ideal which means that $p_3^2 \in e_{Cl(S)}$ so that $o(\overline{p_3}) = 2$ in the class group (where $\overline{p_3}$ is the equivalence class of p_3 in Cl(S)).

   (b) I claim $(y) = (x,y)(x-5,y)(x+5,y)$. Then, note $(x,y), (x-5,y)$, and $(x+5,y)$ are all maximal ideals by the information at the top of the homework, and of course, all maximal ideals are prime. So, I need to show $(y) \subseteq (x,y)(x-5,y)(x+5,y)$ and $(x,y)(x-5,y)(x+5,y) \subseteq (y)$. Well, clearly $(x,y)(x-5,y)(x+5,y) \subseteq (y)$ since $(x,y)(x-5,y)(x+5,y) = (x(x-5)(x+5), x(x-5)y, x(x+5)y, (x-5)(x+5)y, y^2(x+5), y^2(x-5), y^2x, y^3) =: I$ and $x(x-5)(x+5) = y^2$ implies that $(x(x-5)(x+5), x(x-5)y, x(x+5)y, (x-5)(x+5)y, y^2(x+5), y^2(x-5), y^2x, y^3) = (y^2, x(x-5)y, x(x+5)y, (x-5)(x+5)y, y^2(x+5), y^2(x-5), y^2x, y^3)$ and we see that y divides every generator so in particular, every generator belongs to (y), thus the ideal generated by these generators is contained in (y). Now, it remains to show that $(y) \subseteq (x,y)(x-5,y)(x+5,y)$. It suffices to show that $y \in (x,y)(x-5,y)(x+5,y)$. Note that $x(x+5)y = (x^2+5x)y = x^2y+5xy \in I$ and $x(x-5)y = (x^2-5x)y = x^2y-5xy \in I$ implies that $x^2y+5xy+x^2y-5xy = 2x^2y \in I$ which implies $x^2y \in I$. Then, note $(x-5)(x+5)y = x^2y-25y \in I$. So, $x^2y-25y-x^2y = -25y \in I$, which implies that $y \in I$ so that $(y) \subseteq I$ and we are done.

   The corresponding relation is $[(x,y)][(x-5,y)][(x+5,y)] = 1$ where 1 is the class of all principal ideals.

   (c) Note, $p_{a,-b} = (x-a, y+b)$. Then, we compute

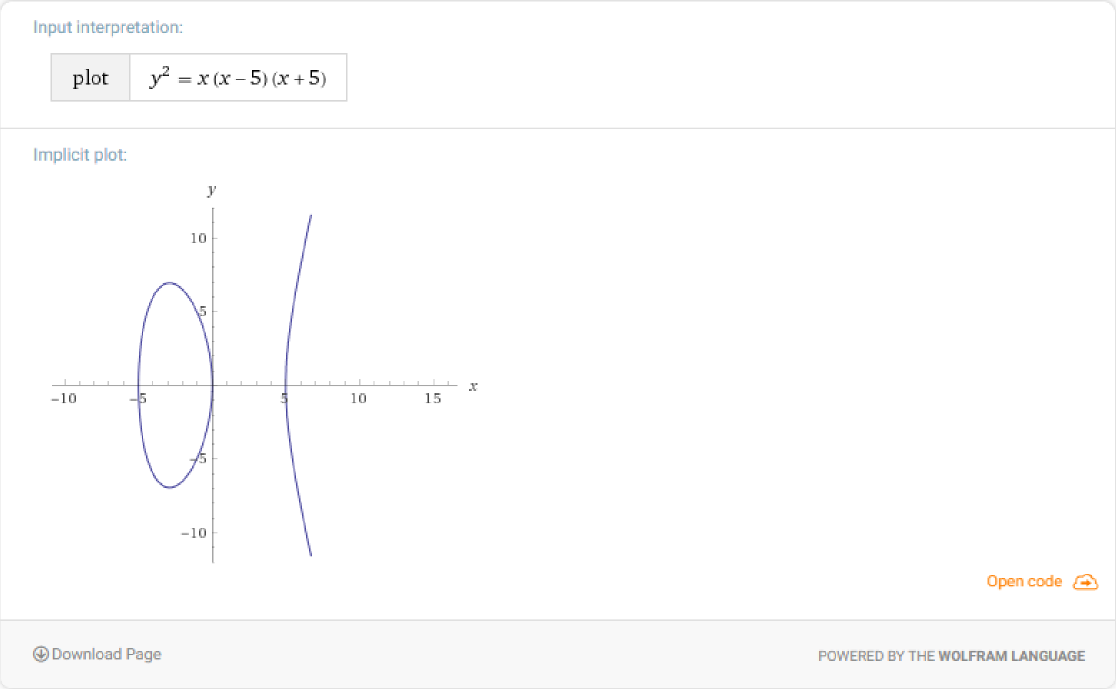
$$\begin{aligned} p_{a,b} * p_{a,-b} &= (x-a, y-b) * (x-a, y+b) \\ &= ((x-a)^2, (x-a)(y+b), (x-a)(y-b), (y-b)(y+b)) \\ &= (x^2-2ax+a^2, xy-ay+bx-ab, xy-ay-bx+ab, y^2-b^2) \end{aligned}$$

   Then, since $xy-ay+bx-ab \in p_{a,b} * p_{a,-b}$ and $xy-ay-bx+ab \in p_{a,b} * p_{a,-b}$ one has that $xy-ay+bx-ab-xy+ay+bx-ab = 2bx-2ab \in p_{a,b} * p_{a,-b}$. Then, if $b \neq 0$, this implies that $x-a \in p_{a,b} * p_{a,-b}$, which implies that $(x-a) \subseteq p_{a,b} * p_{a,-b}$.

   Furthermore, note that $y^2-b^2 = x(x-5)(x+5)-a(a-5)(a+5) = x^3-25x-a^3+25a = x^3-a^3-25(x-a) = (x-a)(x^2+ax+a)-25(x-a) = (x-a)(x^2+ax+a-25)$. So, now one has that $(x-a)$ divides y^2-b^2. Also, $(x-a)$ divides every other generator of $p_{a,b} * p_{a,-b}$, which means that every generator belongs to $(x-a)$. So, $p_{a,b} * p_{a,-b} \subseteq (x-a)$ and in particular $p_{a,b} * p_{a,-b} = (x-a)$ is a principal ideal. So, $p_{a,b} * p_{a,-b} \in e_{Cl(S)}$.

   Now, to show $\overline{P_{a,b}}^{-1} = \overline{P_{a,-b}}$ we must show that for all $I \in \overline{P_{a,b}}$, there exists $J \in \overline{P_{a,-b}}$ such that IJ is a principal ideal. Now, $I \in \overline{P_{a,b}}$ implies that $qI = p(x-a, y-b)$ for some $p, q \in S \setminus \{0\}$. Then, note that setting $J = (x-a, y+b)$ gives $(x-a, y-b)J = (x-a)$. So, $qIJ = p(x-a, y-b)J = p(x-a)$. So, $IJ \sim (x-a)$ (or equivalently $\overline{IJ} = \overline{I} * \overline{J} = \overline{(x-a)} = e_{Cl(S)}$) implies that IJ is a principal ideal and we are done. So, $\overline{I}^{-1} = \overline{P_{a,b}}^{-1} = \overline{J} = \overline{P_{a,-b}}$, which concludes the proof.

   (d) See figure below.



Input interpretation:

plot $y^2 = x(x-5)(x+5)$

Implicit plot:

Open code

Download Page

POWERED BY THE WOLFRAM LANGUAGE

P_1, P_2, P_3 maximal ideals and $P_1 + P_2 + P_3 \supsetneq P_1, P_2, P_3$ implies that $P_1 + P_2 + P_3 = R = (1)$ which is a principal ideal and therefore a representative of the unit element (equivalence class) in the class group.

2. NOTE: throughout my proofs in this problem I am heavily using the fact that all irreducible elements are prime in any UFD.

   We first show that $R[y]$ is integrally closed. Assume not. Assume that there is some element in the fraction field but not $R[y]$ which satisfies some monic polynomial with coefficients in $R[y]$. Very important: one notes that $\mathbb{C}$ a UFD implies that $\mathbb{C}[x]$ is a UFD as is $\mathbb{C}[x][y]$. So, the notion of a GCD makes sense in $R[y]$. Now, take some element $\frac{p}{q} \in Frac(R[y])$ where $p, q \in R[y]$ such that $GCD(p,q) \in R[y]^\times$ (kind of like saying the GCD is 1, we're saying it's a unit). In particular if $GCD(p,q) \notin R[y]^\times$ then say $r :\in GCD(p,q)$. Now, $R[y]$ a UFD implies that we have factorizations $p = u \prod_{i \in I} p_i^{e_i}$ and $q = v \prod_{i \in I} p_i^{d_i}$ into irreducibles p_i where $e_i, d_i \in \mathbb{N}$ (but to be clear some d_i, e_i may be zero) and $u, v \in R[y]^\times$ are some units. Also, NONE of the p_i and p_j are ASSOCIATED for $i \neq j$. Then, $r = w \prod_{i \in I} p_i^{c_i}$ where $c_i \leq min\{e_i, d_i\}$ and $u \in R[y]^\times$ is some unit. Then, let $p' := uw^{-1} \prod_{i \in I} p_i^{e_i - c_i}$ and $q' := vw^{-1} \prod_{i \in I} p_i^{d_i - c_i}$. Now, I claim every common divisor of p' and q' is a unit. Why? Assume not, assume there exists some $r' \in R \setminus R^\times$ so that $r' \mid p'$ and $r' \mid q'$. By definition a GCD is a common divisor of p, q such that every other common divisor divides it. Also, we need to use factorization into irreducibles. So, namely, say that $r' = y \prod_{i \in I} p_i^{b_i}$ where y is some unit. So, in particular $b_i \leq min\{e_i - c_i, d_i - c_i\}$ and $b_i > 0$ for some i. Say $b_j > 0$. Then, note that $p_j^{c_j + b_j} \mid p$ and $p_j^{c_j + b_j} \mid q$. However, this provides a contradiction as it says $p_j^{c_j + b_j}$ is a common divisor of p and q. However, $p_j^{c_j + b_j} \nmid r$ does not divide our chosen GCD, a contradiction. Thus, such an r' does not exist (namely all the b_i's must be zero is what we formally proved). So, now any GCD of p', q' is a unit. We can always use such a procedure to get p', q' whose GCD is a unit. Call those p, q.

   So, we are assuming for contradiction that $\frac{p}{q} \in Frac(R[y])$ satisfies some monic polynomial, f, with coefficients in $R[y]$. Say

   $$f(z) = z^N + \sum_{i=0}^{N-1} g_i z^i$$

   where $g_i \in R[y]$. So, in particular, we have that

   $$\begin{aligned} f(\frac{p}{q}) &= \frac{p}{q}^N + \sum_{i=0}^{N-1} g_i (\frac{p}{q})^i \\ &= 0 \end{aligned}$$

   so that

   $$-(\frac{p^N}{q^N}) = \sum_{i=0}^{N-1} g_i \frac{p^i}{q^i}$$

which implies

$$
\begin{aligned}
-p^N &= \sum_{i=0}^{N-1} g_i \frac{p^i q^N}{q^i} \\
&= \sum_{i=0}^{N-1} g_i p^i q^{N-i}.
\end{aligned}
$$

So, namely one sees that $q \mid$ RHS, which implies that q |LHS. However, $\frac{p}{q} \notin R[y]$ means that the denominator $q \notin R[y]^{\times}$ is NOT a unit. So, now one has $q \mid -p^N$. We have factorizations

$$
\begin{aligned}
q &= u \prod_{i \in I} q_i^{a_i} \\
-p^N &= w \prod_{i \in I} q_i^{s_i} \\
&= w' (\prod_{i \in I} q_i^{h_i})^N \\
&= w \prod_{i \in I} q_i^{N h_i}
\end{aligned}
$$

where we have chosen q_i such that $q_j \not\sim q_k$ for all $k \neq j$ (where $\sim$ means associated) and u, w units and some a_i, s_i, h_i may be zero.
In particular, now we have $a_i \leq s_i = N h_i$. I would like to show for contradiction that p, q have some non-unit common divisor. Take $j \in I$ so that $a_j \neq 0$. Now, if $a_j \leq h_j$, then $p_j^{a_j}$ is a non-unit common divisor of p, q providing a contradiction and we are happy. Otherwise, one has that $a_j > h_j$. However, the fact that $q \mid -p^N$ means that still $a_j \leq s_j = N h_j$. So, $h_j < a_j \leq N h_j$. Then, let $m = max\{m \in \mathbb{N} | m h_j < a_j\}$. Then, however, then that implies that $p_j^{a_j - m h_j}$ is a common divisor of p, q (with $a_j - m h_j \neq 0$ and $a_j - m h_j \leq min\{a_j, h_j\}$), also a contradiction.

So, this completes the proof that such an element $\frac{p}{q} \in Frac(R[y]) \setminus R[y]$ does not exist. So, namely $R[y]$ is integrally closed.

Now, to show that $R[y]$ is not of height 1, we need to give two non-zero prime ideals P_1, P_2 such that $P_1 \subsetneq P_2 \subsetneq R$. Take $P_1 = (y)$ and $P_2 = (x, y)$. Clearly $P_1, P_2 \neq 0$. Also, $P_2 \neq R$ since $1 \notin P_2$. Also, P_2 prime because elements of P_2 are of the form $p(x, y)$ with constant term zero. If I multiply any two polynomials in the complement of P_2 the constant term of the product will remain non-zero since $\mathbb{C}$ is an integral domain. So, the product will remain out of P_2, which means P_2 is prime (prime iff complement closed under product). Also, P_1 is prime since it is generated by y which is irreducible and in a UFD all irreducible elements are prime. Finally, $P_1 \neq P_2$ since $x \in P_2 \setminus P_1$.

To show $R[y]/(y^2 - x^3)$ is an integral domain it suffices to show that $(y^2 - x^3)$ is a prime ideal in $R[y]$. Now, $\mathbb{C}$ a field implies that $R[y] \cong \mathbb{C}[x][y]$ is UFD. Since in a UFD any irreducible element is prime it suffices to show that $y^2 - x^3$ is irreducible. Assume not. Then there exist $p(x), q(x) \in \mathbb{C}[x]$ such that $y^2 - x^3 = (y - p(x))(y - q(x)) = y^2 - y(p(x) + q(x)) + p(x)q(x)$. Now, that implies that $p(x) = -q(x)$, so that $(y - p(x))(y - q(x)) = y^2 - p^2(x) = y^2 - x^3$. However, then that implies that $p(x)^2 = x^3$ a contradiction. So, $y^2 - x^3$ is irreducible and therefore prime which means $R[y]/(y^2 - x^3)$ is an integral domain.

Note, that S is integral over R since we are adjoining root α satisfying $\alpha^2 - x^3 = 0$ a monic polynomial with coefficients in R. Then, assume for contradiciton S has height ≥ 2. Then, there exist prime ideals $0 \subsetneq P_1 \subsetneq P_2 \subsetneq S$. Then, consider $Q_1 = P_1 \cap R$ and $Q_2 = P_2 \cap R$, which are both prime ideals in R. Also, $P_1 \subsetneq P_2$ implies that $Q_1 \subseteq Q_2$. However, then recall that $R = \mathbb{C}[x]$ is a PID, and that all prime ideals are maximal. Thus, $Q_1 = Q_2$. I used this resource which showed that (Proposition 2.2.1) If I have a ring R and S integral over R and prime ideals $0 \subsetneq P_1 \subsetneq P_2 \subsetneq S$ that lie over the same prime (and MAXIMAL) ideal $P = P_1 \cap R = P_2 \cap R$, then $P_1 = P_2$. `https://faculty.math.illinois.edu/~r-ash/ComAlg/ComAlg2.pdf`

S is not integrally closed since there exists $f \in Frac(S) \setminus S$ integral over S. Namely, take $f = \frac{y}{x} + (y^2 - x^3)$. Then, f satisies the following monic polynomial $g \in S[x]$. Take $g(t) = t^3 - (y + (y^2 - x^3))$. (I know I'm writing things in a weird way, but I mean we're in a quotient ring so every element of S is of the form $w + (y^2 - x^3)$ so I'm just being pedantic) So, f is integral. However, $f \notin S$. The integral closure is $S[\frac{y}{x} + (y^2 - x^3)]$. Call $t := \frac{y}{x} + (y^2 - x^3)$.

Also, I claim $\mathbb{C}[t] \cong S[\frac{y}{x} + (y^2 - x^3)]$. Why? Well, $S[\frac{y}{x} + (y^2 - x^3)] \cong \mathbb{C}[x, y, \frac{y}{x}]/(y^2 - x^3) \cong \mathbb{C}[x, y, t]/(y^2 - x^3, xt - y)$. We construct a map $\phi : \mathbb{C}[x, y, t] \to \mathbb{C}[t]$. Namely, $\phi(x) = t^2$, $\phi(y) = t^3$, $\phi(t) = t$ and $\phi(c) = c$ for all $c \in \mathbb{C}$. Then, $ker(\phi) = (y^2 - x^3, xt - y)$, which implies that $\mathbb{C}[t] \cong \mathbb{C}[x, y, t]/(y^2 - x^3, xt - y)$. Finally, note that $Frac(S) \cong \mathbb{C}(t)$ and $S[\frac{y}{x} + (y^2 - x^3)] \cong \mathbb{C}[t]$. Noting that $\mathbb{C}[t]$ is integrally closed in $\mathbb{C}(t)$ (since any PID is integrally closed) one has that $S[\frac{y}{x} + (y^2 - x^3)]$ is integrally closed in $Frac(S)$ and since $S \subseteq S[\frac{y}{x} + (y^2 - x^3)]$ that means that $S[\frac{y}{x} + (y^2 - x^3)]$ is the integral closure of S in its fraction field. `http://mathworld.wolfram.com/IntegrallyClosed.html` `https://math.stackexchange.com/questions/1346738/find-the-integral-closure-of-an-integral-domain-i` `noredirect=1&lq=1` `https://math.stackexchange.com/questions/744356/show-ker-phi-is-a-princip`

3. (a) It suffices to show that all prime ideals are principal. Why? Well, in a Dedekind domain any ideal can be factored as a product of powers of prime ideals. So, assuming all prime ideals (of which there are finitely many) are principal, one then takes an arbitrary ideal I and notes

$$\begin{aligned} I &= \prod_{i=1}^{r} P_i^{e_i} \\ &= \prod_{i=1}^{r} (x_i)^{e_i} \\ &= \prod_{i=1}^{r} (x_i^{e_i}) \\ &= (\prod_{i=1}^{r} x_i^{e_i}) \end{aligned}$$

and we see that I is principal with generator $\prod_{i=1}^{r} x_i^{e_i}$.

So, now we aim to show that all prime ideals are principal. The fact that there are only finitely many prime ideals allows for a useful application of the Chinese Remainder Theorem. Namely, consider the natural projection map

$$\pi : R \to (R/P_1^2) \times (R/P_2) \times \cdots \times (R/P_r).$$

It is surjective meaning that in particular there exists $s \in R$ such that

$$\begin{aligned} \pi(s) =: (\pi_1(s), \pi_2(s), \ldots, \pi_r(s)) && = (p_1^* + P_1^2, 1 + P_2, \ldots, 1 + P_r). \end{aligned}$$

where $p_1^* \in P_1 \setminus P_1^2$ (obviously the CRT only guarantees that $\pi_1(s) = p_1^* + P_1^2$ and as a small point note that there may exist $p_1^{**} \in P_1 \setminus P_1^2$ with $p_1^{**} \neq p_1^*$ such that $p_1^{**} + P_1^2 = p_1^* + P_1^2$). Anyhow, one then considers the principal ideal (s). It has some prime factorization

$$(s) = \prod_{i=1}^{r} P_i^{e_i}.$$

Then, recall $p_1^* \notin P_1^2$ but $p_1^* \in P_1$, which implies that $s \in P_1$ but $s \notin P_1^2$. Also, $\pi_k(s) = 1 + P_k \neq P_k$ for all $k \in \{2, \ldots, r\}$ implies that $s \notin P_k$ for all $k \in \{2, \ldots, r\}$. Then, recall that there is some relation between containment and division. Namely, one has that $(s) \subseteq P_1$, $(s) \nsubseteq P_1^2$, and $(s) \nsubseteq P_k$ for all $k \in \{2, \ldots, r\}$. In particular, this means that $P_1 | s$, but $P_1^2 \nmid (s)$ and $P_k \nmid (s)$ for all $k \in \{2, \ldots, r\}$. So, $e_1 = 1$ and $e_k = 0$ for all $k \neq 1$. So, finally

$$(s) = P_1$$

and we have shown P_1 is principal. By renaming any other prime ideal P_j as P_1, we have shown that all prime ideals are principal, which concludes the proof that all ideals in this domain are principal.

(b) Take any $\alpha \in I \setminus \{0\}$. Now, say I has prime factorization

$$I = \prod_{i=1}^{n} P_i^{e_i}$$

Now, $\alpha \in I$ implies that $(\alpha) \subseteq I$ which also implies that $I \mid (\alpha)$. So, namely

$$(\alpha) = \prod_{i=1}^{n} P_i^{d_i} \prod_{j=1}^{m} Q_j^{c_j}$$

where $d_i \geq e_i$ for all $i \in [n]$ and $c_j \in \mathbb{N}$.

Now, intuitively (this is not a proof, just a little intuition before I jump into the details) if some element β is in I but not in (α) that is because $(\beta) = \prod_{i=1}^{n} P_i^{l_i} \prod_{j=1}^{m} Q_j^{h_j} \prod_{k=1}^{t} M_k^{b_k}$ where there exists some $i \in [n]$ such that $l_i < d_i$ or there exists some $j \in [m]$ such that $h_j < c_j$.

Now, we apply the CRT to the following projection map

$$\pi : R \to R/P_1^{e_1+1} \times R/P_2^{e_2+1} \times \cdots \times R/P_n^{e_n+1} \times R/Q_1 \times \cdots \times R/Q_m.$$

First, for all $i \in [n]$, pick $p_i^* \in P_i^{e_i} \setminus P_i^{e_i+1}$. The CRT guarantees the existence of $s \in R$ such that $\pi_{P_i^{e_i^1}}(s) = p_i^* + P_i^{e_i+1}$ for all $i \in [n]$ and such that $\pi_{Q_j} = 1 + Q_j$ for all $j \in [m]$. So, this implies that $s \in P_i^{e_i} \setminus P_i^{e_i+1}$ for all $i \in [n]$ and $s \notin Q_j$ for all $j \in [m]$.

So, we have some prime factorization

$$(s) = \prod_{i=1}^{n} P_i^{e_i} \prod_{j=1}^{m} Q_j^0 \prod_{k=1}^{t} M_k^{b_k}.$$

Now, take arbitrary $i \in I$, we wish to show that there exist $j, k \in R$ such that $i = j\alpha + ks$. So, consider the projection map

$$\phi : R \to\to R/P_1^{d_1} \times R/P_2^{d_2} \times \cdots \times R/P_n^{d_n} \times R/Q_1^{c_1} \times \cdots \times R/Q_m^{c_m}.$$

Then, compute $\phi(i)$. If $\phi(i) = 0$, then $i \in (\alpha)$. Otherwise, some work remains.

We actually reduce via another projection map which will guarantee an element w such that $w \equiv i \bmod (\alpha)$ and $w \equiv 0 \bmod (s)$.

$$\phi^* : R \to\to R/P_1^{d_1} \times R/P_2^{d_2} \times \cdots \times R/P_n^{d_n} \times R/Q_1^{c_1} \times \cdots \times R/Q_m^{c_m} \times R/M_1^{b_1} \times \cdots \times R/M_t^{b_t}.$$

Then, for all $i \in [n]$ let $\tilde{p}_i \in P_i^{e_i} \cap (\pi_{P_i^{d_i}}(i) + P_i^{d_i})$ and let $\tilde{q}_j \in \pi_{Q_j^{c_j}} + Q_j^{c_j}$. Then, the CRT guarantees the existence of an element $w \in R$ such that $\phi^*(w) = (\tilde{p}_1 + P_1^{d_1}, \tilde{p}_2 + P_2^{d_2}, \ldots, \tilde{p}_n + P_n^{d_n}, \tilde{q}_1 + Q_1^{c_1}, \tilde{q}_2 + Q_2^{c_2}, \ldots, \tilde{q}_m + Q_m^{c_m}, 0, 0, \ldots, 0)$. So, namely, one has that $w \equiv i \bmod (\alpha)$ and $w \equiv 0 \bmod (s)$. So, there exist $j, k \in R$ such that $w = i + j\alpha$ and $w = ks$. So, $i = ks - j\alpha$ and we are done.