Math 6122: HW 6

Padmavathi Srinivasan

Due: Friday, Mar 15th, 5:00 P.M.

1. Let $d \geq 2$ be a square-free integer and let $K = \mathbb{Q}(\sqrt{-d})$. Compute $\mathcal{O}_K$ and the multiplicative units in the ring $\mathcal{O}_K$.

2. Show that the ideal $\mathcal{P} = (2, 1 + \sqrt{-3})$ is a prime ideal in the ring $\mathbb{Z}[\sqrt{-3}] = \mathbb{Z}[x]/(x^2 + 3)$. Verify that $\mathcal{P}^2 = 2\mathcal{P}$ but $\mathcal{P} \neq (2)$. Why does this not contradict unique factorization of ideals into product of prime ideals?

3. Show that a PID that is not a field is a Dedekind domain.

4. Show that a Dedekind domain is a PID if and only if it is a UFD.

5. Find compatible $\mathbb{Z}$-bases for $\mathbb{Z}[i]$ and the ideal $(1+i)$, i.e. find α_1 and α_2 in $\mathbb{Z}[i]$ such that $\mathbb{Z}[i] = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2$ such that $(1 + i)\mathbb{Z}[i] = \mathbb{Z}(2\alpha_1) + \mathbb{Z}\alpha_2$. Use these bases to show that there is a fundamental domain for $\mathbb{C}/(1+i)\mathbb{Z}[i]$ (namely the region $S_{(1+i)} = \{2r_1\alpha_1 + r_2\alpha_2 \mid 0 \leq r_1, r_2 \leq 1\}$) can be tiled using two translates of the fundamental domain for $\mathbb{C}/\mathbb{Z}[i]$ (namely the region $S = \{r_1\alpha_1 + r_2\alpha_2 \mid 0 \leq r_1, r_2 \leq 1\}$). Draw a picture. What is the relation to $N_{\mathbb{Q}(i)/\mathbb{Q}}(1 + i) = 2$? (Reading and understanding the proof of Theorem A.11 in the book might be helpful for this exercise if you cannot guess the correct answer. This is a change of basis algorithm but for integral lattices in place of vector spaces.)

6. 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 $R = \mathbb{C}[x]$. Show that the integral closure S of R in E is $R[y]/(p(y))$. Show that S is a Dedekind domain. (Hints: For Noetherian, you may use the fact polynomial rings over Noetherian rings are Noetherian and that the quotient of a Noetherian ring by an ideal is Noetherian. For showing S is integrally closed, mimic the proof of problem 1 with $\mathbb{Z}$ replaced by $\mathbb{C}[x]$ and the squarefree integer d replaced by the squarefree polynomial $x(x - 5)(x + 5)$. Show that the inverse image $\varphi^{-1}(\mathcal{P})$ of a nonzero prime ideal $\mathcal{P}$ of S under the map $\varphi\colon \mathbb{C}[x] \to S$ is a nonzero prime ideal of $\mathbb{C}[x]$, and therefore of the form $(x - a)$ for some $a \in \mathbb{C}$. Then use this to show $\mathcal{P} = (x - a, y - b)$ for $b \in \mathcal{C}$ such that $b^2 = a(a - 5)(a + 5)$. Conclude that $\mathcal{P} \to \varphi^{-1}(\mathcal{P})$ is a $2 : 1$ surjective map from prime ideals of S to prime ideals of $\mathbb{C}[x]$ except over the ideals $(x), (x-5), (x+5)$. It is a "$2 : 1$ branched covering map" – can you draw a picture of the prime ideals?)

Math 6122 - Homework 6

Caitlin Beecham ()

March 15, 2019

1

Say we have $\omega \in O_K$. Namely, $\omega \in Q(\sqrt{-d})$ such that there exists monic $f(x) \in Z[x]$ such that $f(\omega) = 0$. Namely, we know $\omega = a + b\sqrt{-d}$ for some $a, b \in Q$. Write $a = \frac{p}{m}$ where $m \neq 0$ and $gcd(p, m) = 1$ (gcd exists since p,q are just integers) and $b = \frac{q}{r}$ with $r \neq 0$ and $gcd(q, r) = 1$. Then, $Q(\sqrt{-d})$ a quadratic extension and the fact that for any $\omega \in Q(\sqrt{-d})$ we have that $Q(\omega) \subseteq Q(\sqrt{-d})$ and the divisibility rule for towers of extensions, we know ω has degree 1 or 2 over Q. If we pick $\omega \notin Q$, it has degree 2. So, it's minimal polynomial is of degree 2. We note

$$\begin{aligned} \omega &= a + b\sqrt{-d} \\ \omega^2 &= a^2 + 2ab\sqrt{-d} + (-b^2 d) \end{aligned}$$

Then, note that

$$\omega^2 - 2a\omega = -a^2 + (-b^2 d) \in Q.$$

So, we have that $m_\omega(x) = x^2 - 2ax + (a^2 + b^2 d)$.

$$\begin{aligned} m_\omega(x) &= x^2 - 2ax + (a^2 + b^2 d) \\ &= x^2 + \frac{-2p}{m}x + (\frac{p^2}{m^2} + \frac{q^2}{r^2}d) \end{aligned}$$

Now, $\omega \in O_K$ (as shown in class) if and only if $m_\omega \in Z[x]$. So, we know that $-2a = \frac{-2p}{m} \in Z$ and $a^2 + b^2 d = \frac{p^2}{m^2} + \frac{q^2}{r^2}d \in Z$. Then, $4a^2 + 4b^2 d \in Z$ and $4a^2 + 4b^2 d = (-2a)^2 + 4b^2 d \in Z$ implies that $4b^2 d \in Z$. Then, $4b^2 d = (2b)^2 d = \frac{4q^2}{r^2} d \in Z$ implies that

So, $\frac{-2p}{m} \in Z$ implies that $m | -2p$ iff there exists $u \in Z$ such that $um = -2p$. Now Z is a UFD, so $um = -2p = (-1)^{e_1} 2^{e_2} p_3^{e_3} \ldots p_k^{e_k}$. Also, 2 divides RHS implies that 2 divides LHS. So, then 2 prime means $2|m$ or $2|u$. If $2|m$, then $m = 2m'$ so that $um = 2um' = -2p$ or $p = -um'$, then $\frac{p}{m} = \frac{-um'}{2m'}$, a contradiction to $gcd(p, m) = 1$ if $m' \notin \{1, -1\}$. So, we get a contradiction unless $m' = \pm 1$ or equivalently $m = 2m' = \pm 2$. If $2|u$ and 2 does not divide m then, $u = 2u'$ so that $2u'm = -2p$ or $u'm = -p$ so then $\frac{p}{m} = \frac{-u'm}{m}$, a contradiction to $gcd(p, m) = 1$ unless $m = \pm 1$. So, we know that unless $m \in \{\pm 1, \pm 2\}$, we certainly get a contradiction. So, one must have that $m \in \{\pm 1, \pm 2\}$.

Next, we recall that $(\frac{p^2}{m^2} + \frac{q^2}{r^2}d) \in Z$. So,

$$\begin{aligned} \frac{p^2}{m^2} + \frac{q^2}{r^2}d &\in \{(\frac{p}{m})^2 + \frac{q^2}{r^2}d : m \in \{\pm 1, \pm 2\}, p, q \in Z, r, d \in Z^\times\} \\ &\subseteq \{(\frac{p'}{2})^2 + \frac{q^2}{r^2}d : p', q \in Z, r, d \in Z^\times\} \end{aligned}$$

where to get from the above line to here we set $p' = p$ if $m = 2$, or $p' = -p$ if $m = -2$, or $p' = 2p$ if $m = 1$ and $p' = -2p$ if $m = -1$.

Continuing on we have

$$\begin{aligned}\frac{p^2}{m^2} + \frac{q^2}{r^2}d &\in \{(\frac{p}{m})^2 + \frac{q^2}{r^2}d : m \in \{\pm 1, \pm 2\}, p, q \in Z, r, d \in Z^\times\} \\ &\subseteq \{(\frac{p'}{2})^2 + \frac{q^2}{r^2}d : p', q \in Z, r, d \in Z^\times\} \\ &\subseteq \{\frac{p'^2}{4} + \frac{q^2}{r^2}d : p', q \in Z, r, d \in Z^\times\}\end{aligned}$$

Then, note that $\frac{p'^2}{4} + \frac{q^2}{r^2}d = \frac{p'^2r^2+4q^2d}{4r^2} \in Z$ implies that $p'^2r^2 + 4q^2d \in (4r^2)Z \subseteq 4Z$ which implies that 4 divides $p'^2r^2 + 4q^2d$ and then 4 divides p'^2r^2

$4r^2$ divides $p'^2r^2 + 4q^2d$. Then, r^2 divides p'^2r^2 and r^2 divides $p'^2r^2 + 4q^2d$ implies that r^2 divides $4q^2d$ or there exists $M \in Z$ such that $Mr^2 = 4q^2d$. Then, $gcd(q, r) = 1$ implies that r^2 divides $4d$ UNLESS $q = 0$. Assume for contradiction $q \neq 0$. So, there exists r' such that $r^2r' = 4d$. Then, by UFDness of Z, 2 divides r' or 2 divides r. If 2 divides r then $r = 2k$ and $r^2 = 4k^2$, and then $r^2 = 4k^2$ divides $4d$ so that $4k^2r' = 4d$ or $k^2r' = d$, but then that's a contradiction to d square free UNLESS $k = 1$ which would imply that $r = 2$. So, 2 does not divide r UNLESS $r = 2$, but then we must have 2 divides r' so $r' = 2k'$ so that $r^2r' = 4d = 2r^2k'$ which gives $2d = r^2k'$. Then UFDness of Z says (and PRIMENESS of 2) 2 divides r or 2 divides k'. We just showed one cannot have 2 divides r UNLESS $r = 2$. So, necessarily, 2 divides k' so that $k' =: k_1 = 2k_2$ for some $k_2 \in Z$. Hence, $2d = r^2k' = 2r^2k_2$ or $d = r^2k_2$. However, then this is a contradiction to d squarefree. So, assuming $q \neq 0$ leads to a contradiction, unless $r = 2$, so $r = 2$.

$$\omega = \frac{p'}{2} + \frac{q'}{2}\sqrt{d} \text{ for some } p', q' \in Z$$

where to get from the above line to here we set $p' = p$ if $m = 2$, or $p' = -p$ if $m = -2$, or $p' = 2p$ if $m = 1$ and $p' = -2p$ if $m = -1$ and similarly for q'.

So, going back to a previous equation $a^2+b^2d = \frac{p'^2}{4}+\frac{q'^2}{4}d \in Z$. Or equivalently, $p'^2+q'^2d \in 4Z$. So, $p'^2 + q'^2d \equiv 0 mod 4$. Cases: $d = 1, 2, 3$ mod 4 (can't have $d = 0$ mod 4 since d squarefree). Say $d = 1$ mod 4. Then, $p'^2 + q'^2 \equiv 0 mod 4$ which means that 4 divides $p'^2 + q'^2$. $p'^2 + q'^2 = 4v$ for some $v \in Z$. This happens exactly when p', q' both even. Otherwise if exactly one is odd, then the sum is odd. IF both are odd we have $(2k+1)^2 + (2h+1)^2 = 4k^2 + 4k + 1 + 4h^2 + 4h + 1 \equiv 2$ mod 4. So, both are even if $d = 1$ mod 4. If $d = 2$ mod 4, then $p'^2 + 2q'^2 \equiv 0$ mod 4. So that if both p', q' even we get $(4k^2 + 2(4h^2) \equiv 0) mod 4$. If both are odd we get $4k^2 + 4k + 1 + 8h^2 + 8h + 2 \equiv 3$ mod 4. If p' even, q' odd then, $4k^2 + 8h^2 + 8h + 2 \equiv 3$ mod 4. If p' odd and q' even then, $4k^2 + 4h + 1 + 4h^2 \equiv 1$ mod 4 a contradiction. If $d = 3$ mod 4, then $p'^2 + q'^2d = p'^2 + 3q'^2 \equiv 0$ mod 4. So, both even gives $p'^2 + q'^2d = 4k^2 + 3(4h^2) \equiv 0 mod 4$, so that works. If both odd we have $4k^2 + 4k + 1 + (3)(4h^2 + 4h + 1) = 4k^2 + 4k + 1 + 12h^2 + 12h + 3 \equiv 0$ mod 4, so that works. If p' even q' odd then $p'^2 + q'^2d = 4k^2 + (3)(4h^2 + 4h + 1) = 4k^2 + 12h^2 + 12h + 3 \equiv 3 mod 4$ so that doesnt work. If p' odd, q' even, then $p'^2 + q'^2d = 4k^2 + 4k + 1 + (3)(4h^2) \equiv 1 mod 4$ so that doesnt work. To summarize: if $d = 1, 2$ mod 4. Then we need both p' and q' even. If $d = 3$ mod 4, we need that $p' = q'$ mod 2.

So, if $d = 1, 2$ mod 4, then

$$\begin{aligned}O_k &\subseteq \{\frac{p'}{2} + \frac{q'}{2}\sqrt{-d} \text{ for some } p', q' \in Z \text{ such that } p' \equiv q' \equiv 0 \text{ mod } 2\} \\ &= \{p'' + q''\sqrt{-d} \text{ for some } p'', q'' \in Z\} \\ &= Z + Z\sqrt{-d}\end{aligned}$$

If $d = 3 \bmod 4$, then

$$\begin{aligned} O_k &\subseteq \{\frac{p'}{2} + \frac{q'}{2}\sqrt{-d} \text{ for some } p', q' \in Z \text{ such that } p' \equiv q' \bmod 2\} \\ &= Z + Z\sqrt{-d} + \frac{1}{2}Z + \frac{1}{2}Z\sqrt{-d} \\ &= \frac{1}{2}Z + \frac{1}{2}Z\sqrt{-d} \end{aligned}$$

Finally, we note that $Z + Z\sqrt{-d} \subseteq O_K$ when $d = 1, 2 \bmod 4$ and $\frac{1}{2}Z + \frac{1}{2}Z\sqrt{-d} \subseteq O_K$ when $d = 3 \bmod 4$. Why? Because given $\omega = a + b\sqrt{-d} \in Z + Z\sqrt{-d}$ (resp $\in \frac{1}{2}Z + \frac{1}{2}Z\sqrt{-d}$), the minimal polynomial $m_\omega(x) = x^2 - 2ax + (a^2 + b^2 d) \in Z[x]$ is an integral polynomial by construction. So those containments are actually equalities.

Now, what are the units in O_K in these cases? They are elements which have inverses in O_K. Say $d = 1, 2 \bmod 4$. Then, take $a + b\sqrt{-d} \in O_K$. What is $(a + b\sqrt{-d})^-1$? Assume it belongs to O_K (it exists in K since K is a field). Then, $(a + b\sqrt{-d})^-1 = c + e\sqrt{-d}$ for some $c, e \in Z$. So, $(a + b\sqrt{-d})(c + e\sqrt{-d}) = ac - bed + (ae + bc)\sqrt{-d} = 1$ implies that $ae + bc = 0$ and $ac - bed = 1$. So, $ac = 1 + bed$ and then either $a = 0$ or $c = \frac{1+bed}{a}$. Then, if $a \neq 0$, we plug in $ad + bc = ae + b(\frac{1+bed}{a}) = 0 = \frac{a^2e+b+b^2e}{a}$ which implies that $a^2e + b + b^2e = 0$ or $e(a^2 + b^2) + b = 0$ or $e(a^2 + b^2) = -b$ and then $a \neq 0$ implies $a^2 + b^2 \neq 0$ so $e = \frac{-b}{a^2+b^2}$. So, if $a \neq 0$, then $c + ei = \frac{1+bed}{a} + \frac{-b}{a^2+b^2}i = (a + bi)^{-1}$. By assumption $c + ei = \frac{1+be}{a} + \frac{-b}{a^2+b^2}i \in O_K$ which means $\frac{1+bed}{a}, \frac{-b}{a^2+b^2} \in Z$. So, $(a^2 + b^2)e = -b$ so $ea^2 + eb^2 = -b$ which means $eb^2 + b + ea^2 = 0$ or $b = \frac{-1 \pm \sqrt{1-4e^2a^2}}{2e}$. Also, $ca = 1 + bed$. Then, $1 + bed = 1 + (-ea^2 - eb^2)ed = ca = 1 - ea^2ed - eb^2ed = -e^2d(a^2+b^2)+1 = -ea^2ed+(1-eb^2ed)$. Now, Z a UFD implies that a divides $1 - b^2e^2d$. So $af = 1 - b^2e^2d$ for some $f \in Z$. Also $ca = 1 + bed$. So, $cabe = be + b^2e^2d$. Then, $ca + fa = 1 + be = (c + f)a = 1 + be$ or $1 + be \equiv 0 \bmod a$. Now, $ca = 1 + bed = 1 + be + be(d-1)$ which gives $be(d-1) \equiv 0 \bmod a$. Then, $be(d-1) = bed - be \equiv -1 - be = -1(1 + be) \equiv 0 \bmod a$. Then, $be \equiv -1 \bmod a$ and $cabe = be + b^2e^2d \equiv -1 + b^2e^2d \equiv 0 \bmod a$ implies that $b^2e^2d \equiv 1 \bmod a$. So, a divides $b^2e^2d - 1$. Namely, $aa' = b^2e^2d - 1$.

Also, if $a \neq 0$, then $e = \frac{-bc}{a}$. So, now $1 + bed = 1 + \frac{-b^2cd}{a} = ca$ and $\frac{-bc}{a} \in Z$. Then, $e = \frac{-b^2cd}{a} \equiv -1 \bmod a$. Also, $ca \equiv 1 \bmod b$ unless a does not divide $-bcd$. So, $e = ca - 1$.

Now, if $b \neq 0$, then $c = \frac{-ae}{b}$. So, if $a, b \neq 0$, then $c = \frac{-ca^2-a}{b}$ or equivalently $cb = -ca^2 - a$ which gives $ca^2 + a + cb = 0$ or $c(a^2 + b) = -a$ or PROVIDED $a^2 + b \neq 0$ (iff $b \neq -a^2$) then $c = \frac{-a}{a^2+b}$ and then $e = \frac{-a^2}{a^2+b} - 1 = \frac{-a^2-b+b}{a^2+b} = -1 + \frac{b}{a^2+b} - 1 = -2 + \frac{b}{a^2+b}$. So, we get that $a^2 + b$ divides both b and a^2. So, there exist $r', r'' \in Z$ such that $r'a^2 + r'b = b$ and $r''a^2 + r''b = a^2$ or $r'a^2 = b(1 - r')$ and $r''b = a^2(1 - r'')$. Then, provided $r'' \neq 0$ and $1 - r' \neq 0$ we have $b = \frac{a^2(1-r'')}{r''} = \frac{r'a^2}{1-r'} = a^2\frac{1-r''}{r''} = a^2\frac{r'}{1-r'}$. So, since we are still assuming $a \neq 0$, we have $\frac{1-r''}{r''} = \frac{r'}{1-r'}$.

Hmmm... here's a resource:

`https://en.wikipedia.org/wiki/Dirichlet\%27s_unit_theorem` so $r = r_1 + r_2 - 1$ where r_1 is number of conjugates of $\sqrt{-d}$ that are real and r_2 is half the number of conjugates which are complex. So, $r_1 = 0$ and $r_2 = 1$. Then, $r = r_1 + r_2 - 1$. So, this has multiplicative rank 0 (we're looking for a multiplicative set of generators for the group of units).

TODO: go ask about this.

2

This is not a contradiction because we used every condition for a Dedekind domain in our proof of unique factorization into prime ideals. So, namely, we only proved the statement for Dedekind domains.

I claim the ring $\mathbb{Z}[\sqrt{-3}]$ is not a Dedekind domain. Namely, I claim that it is not integrally closed. Namely, one notes that $S := \{\alpha \in Frac(\mathbb{Z}[\sqrt{-3}]) : f(\alpha) = 0 \text{ for some monic } f(x) \in \mathbb{Z}[\sqrt{-3}][x]\} \supsetneq \mathbb{Z}[\sqrt{-3}]$. We show that this inclusion is proper by producing some $\alpha \in S \backslash \mathbb{Z}[\sqrt{-3}]$. Namely, take the monic polynomial $f(x) = x^2 + (2+2\sqrt{-3})x + (-2-\sqrt{-3})$. The quadratic formula tells us a root is $\alpha = \frac{-2-2\sqrt{-3}+\sqrt{4+4\sqrt{-3}-12+4*2+4\sqrt{-3}}}{2} = \frac{-2-2\sqrt{-3}+\sqrt{8\sqrt{-3}}}{2} = -1-\sqrt{-3}+\sqrt{2}(-3)^{\frac{1}{4}}$. Now, $\alpha \in Z[\sqrt{-3}]$ if and only if $\sqrt{2}(-3)^{\frac{1}{4}} \in Z[\sqrt{-3}]$ (because $-1-\sqrt{-3} \in Z[\sqrt{-3}]$). However, $\sqrt{2}(-3)^{\frac{1}{4}} \notin Z[\sqrt{-3}]$ which means that we have produced $\alpha \in S\backslash Z[\sqrt{-3}]$, which means that $Z[\sqrt{-3}]$ is not integrally closed and thus not a Dedekind domain. We only proved unique factorization of ideals into prime ideals for Dedekind domains.

3

Show that any PID, R, that is not a field is a Dedekind domain.

We need to show (1) R Noetherian, (2) R is height 1, (3) R integrally closed.

(1) Equivalently, one needs to show that every ideal is finitely generated. In a PID every ideal is principal and therefore finitely generated.

(2) We need to show that every non-zero prime ideal is maximal, and that there exist non-zero prime ideals. To start, we wish to show existence of a non-zero prime ideal. Take an irreducible element $x \in R$. I first show that it generates a prime ideal.

$$I := \langle x \rangle$$

Say $yz \in I$. Then, I wish to show that $y \in I$ or $z \in I$. Well, $yz \in I$ if and only if $yz = cx$ for some $c \in R$. Now, R a PID implies that R is a UFD. So, any two different factorizations differ by units and reordering only. So, (WLOG, about the reordering part; we can just rename y and z if the order is switched) there exist units $u, v \in R$ such that $y = cu$ and $z = vx$. Then, $z = vx$ implies that $z \in I$ and we are done. So, any irreducible element generates a non-zero prime ideal. (Also, irreducible elements exist since a PID is a UFD and in a UFD any element factors as a product of irreducibles).

Now, we need to show that every non-zero prime ideal is maximal. Take a non-zero prime ideal I. Since R is a PID, we know that there exists $x \in R$ such that $I = \langle x \rangle$. Now, I prime implies that whenever $yz \in I$, $y \in I$ or $z \in I$. Now, we wish to show that if J is an ideal such that $I \subseteq I \subseteq J \subseteq R$ and $I \neq J$, then $J = R$. We know there exists $w \in R$ such that $J = \langle w \rangle$ since this ring is a PID. Now, $I \subseteq J$ if and only if w divides x. So, there exists $c \in R$ such that $x = cw$. Now, $x \in I$ and I a prime ideal implies that $c \in I$ or $w \in I$.

However, we know that $w \notin I$. Why? Otherwise if $w \in I$, then that means that x divides w, but then we have the fact that x divides w AND w divides x so that namely, there exist $c, d \in R$ such that $w = cx$ and $x = dw$. Then, that implies $w = cdw$ or $w(1-cd) = 0$, but then R a PID implies that R is an integral domain (by definition), so then $I \neq 0$ implies $J \neq 0$ implies $w \neq 0$ which implies that $cd = 1$ so that c, d are units (and inverses of each other) in R. So, really $c = d^{-1}$. Then, $I = \langle x \rangle = \langle dw \rangle$ and $RI = I$ means that $d^{-1}I \subseteq I$ but $d^{-1}dw = w \in d^{-1}I \subseteq I$. Now, we have that $w \in I$, but then that implies that $J = \langle w \rangle \subseteq I$, which together with $I \subseteq J$ means that $I = J$, a contradiction. So, $w \notin I$.

Then, that means that $c \in I$ which means that x divides c. So, there exists $d \in R$ such that $c = xd$. Then, we recall that $x = cw = xdw$, which means that $x(1 - dw) = 0$, and since $I \neq 0$, $x \neq 0$, which means that (since R is an integral domain) $1 = dw$. Now, J an ideal means that $JR = J$ and in particular that $dJ = w^{-1}J = w^{-1}\langle w \rangle \subseteq J$, which implies that $ww^{-1} = 1 \in J$, but then $JR \subseteq J$ and $1 \in J$ implies that $J = R$ and we are done with (2).

(3) Finally, we need to show that R is integrally closed. Namely, that if $K = Frac(R)$, then we need to show that $O_K = R$. What is O_K? Well,

$$O_K = \{\alpha \in K : \text{ there exists } f \in R[x] \text{ monic such that } f(\alpha) = 0\}.$$

Namely, we need to show that $O_K \subseteq R$ and $R \subseteq O_K$. Clearly, $R \subseteq O_K$, since for any $r \in R$ the polynomial $f(x) = x - r \in R[x]$ is monic and has r as a root. Then, it remains to show that $O_K \subseteq R$. We assume for contradiction that there exists $\alpha \in O_K \setminus R$ or equivalently that there exists $\alpha \in K \setminus R$ with polynomial $f \in R[x]$ monic such that $f(\alpha) = 0$. So, $\alpha in Frac(R) \setminus R$. That means there exist $p, q \in R$ such that $\alpha = \overline{(p,q)} \in Frac(R)$. Now, R a UFD implies that $y := gcd(p,q)$ exists (it may not be unique). Then, let $p' = py^{-1}$ and $q' = qy^{-1}$. Now $\alpha = \overline{(p,q)} = \overline{(p',q')}$ since by the equivalence relation which defines $Frac(R)$ we have $(p,q) \sim (p',q')$ if and only if $pq' = qp'$. So, we verify $pq' = pqy^{-1} = qp'$ which means that $\overline{(p,q)} = \overline{(p',q')}$.

We recall the definition of a gcd. If $y = gcd(p,q)$, then for any common divisor w with $w|p$ and $w|q$, one has that $w|y$.

Ok, now, one has that $f(\alpha) = 0$. Say that

$$f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$$

where $a_i \in R$ for all i. So, we see that

$$f(\alpha) = \alpha^n + \sum_{i=0}^{n-1} a_i \alpha^i$$

Now, $f((p',q')) \in f(\alpha)$ (here I am thinking of $f(\alpha)$ as the (element of Frac(R)) or equivalence class of $R \times R$ containing (p',q')). Then, the polynomial $\hat{f}(p',q') \in R \times R[x]$ satisfies

$$\hat{f}((p',q')) = (p',q')^n + \sum_{i=0}^{n-1} a_i (p',q')^i,$$

and

$$(q',1)^n \hat{f}((p',q')) = (p',1)^n + \sum_{i=0}^{n-1} a_i (q'^{n-i} p^i, 1).$$

Then, one considers the polynomial $g(x) \in R[x]$ defined by

$$g(x) = x^n + \sum_{i=0}^{n-1} a_i q'^{n-i} x^i.$$

One sees that $g(p') = 0$. In particular, $p'^n = -\sum_{i=0}^{n-1} a_i q'^{n-i} p'^i$ which means that $q'|p'^n$. Now, we show $gcd(p',q') = 1$.

(Why? Well, say not, say $gcd(p',q')$ is not a unit for any gcd (any gcd being a unit is what we really mean by gcd = 1 (since gcds are only unique up to units)). Then, any common divisor u of

p' and q' is not a unit. Say $u|p'$ and $u|q'$ where u is not a unit. Then, $p' = mu$ and $q' = nu$. Recall $p' = py^{-1} = mu$ and $q' = qy^{-1} = nu$. Then, $p = muy$ and $q = nuy$ implies that uy is a common divisor of both p and q, but then by the definition of a gcd, $uy|y$, so that $y = xuy$) that means that $xu = 1$, so that $u \in R^\times$ is a unit, a contradiction. So, $gcd(p', q') = 1$ (all the gcds are units, in particular 1 is one of the gcds)).

Now, since $gcd(p', q') = 1$, the fact that $q'|p'^n$ implies that $q'|p'$. But then $q'|q', p'$ implies that q' is a common divisor, but then by the definition of a gcd, if $1 = y' = gcd(p', q')$, then for any common divisor w with $w|p'$ and $w|q'$, one has that $w|y' = 1$. So, $q'|1$ which implies that q' is a unit, but then (p', q') can be embedded canonically into R as $p'q'^{-1}$, which means that in fact $\alpha \in R$, so we see that R is integrally closed since for any $\alpha \in O_K$, we have that $\alpha \in R$. Thus, R is a Dedekind domain.

4

Show that a Dedekind domain is a PID if and only if it's a UFD. `https://en.wikipedia.org/wiki/Unique_factorization_domain` Well, any PID is a UFD. Now it remains to show that any Dedekind domain which is a UFD is a PID. Well,

Lemma (1): In a Dedekind domain which is a UFD, every (height one) prime ideal is principal.

Proof: Say $I \subseteq R$ is a prime ideal. Namely, this means that $xy \in I$ implies that $x \in I$ or $y \in I$. Now, R Noetherian implies that every ideal is finitely generated. So, $I = \langle x_1, x_2 \ldots, x_k \rangle$. Now, consider $I_j = \langle x_j \rangle$. Clearly, $\bigcap_{j \in [k]} I_j = \langle x_1 x_2 x_3 \ldots x_k \rangle$. We then note that $\langle x_1 x_2 x_3 \ldots x_k \rangle \subseteq I$. Clearly, $I_1 \subseteq I$. Is I_1 prime? Well, it's prime if and only if for all $xy \in I_1$ one has $x \in I_1$ or $y \in I_1$. Clearly, if x_1 is irreducible, then since R is a UFD, it is also prime, which means I_1 is a prime ideal.

So, say x_1 is reducible, namely $x_1 = y_1 z_1$ for $y_1, z_1 \in R \setminus R^\times$. Without loss of generality, one may assume that y_1 is irreducible.

(Otherwise,

- Initialize $y_1^0 := y_1$;
- While y_1^i is reducible:
  - Then $y_1^i = y_2^i y_3^i$ for some non-units y_2^i, y_3^i.
  - Update $z_1^{i+1} := z_1^i y_3^i$;
  - Update $y_1^{i+1} := y_2^i$;
  - Update $i := i + 1$;

Then, one knows this process will eventually stop. Why? If it doesn't, we have constructed an infinite chain of strictly increasing ideals $\langle y_1^0 := y_1 \rangle \subseteq \langle y_1^1 \rangle \subseteq \langle y_1^2 \rangle \subseteq \langle y_1^3 \rangle \cdots \subseteq \langle y_1^i \rangle \subseteq \langle y_1^{i+1} \rangle \ldots$ but then since R is Noetherian, every ascending chain stabilizes, which gives us a contradiction).

So, we have $x_1 = y_1 z_1$ with y_1 irreducible. Then, $x_1 = y_1 z_1 \in I$ and I prime implies that $y_1 \in I$ or $z_1 \in I$.

Case (1): Say that $y_1 \in I$. Then, $\langle x_1 \rangle \subseteq \langle y_1 \rangle \subseteq I$. Now, y_1 irreducible implies that y_1 is prime since R is a UFD which means $\langle y_1 \rangle$ is a prime ideal which is also non-zero (since $x_1 = y_1 z_1$ and R is an integral domain). Now, R height 1 implies that $\langle y_1 \rangle = I$ which means that I is principal and we're done.

Case (2): $z_1 \in I$ and $y_1 \notin I$. Then, still $\langle y_1 \rangle$ is a prime ideal and $\langle x_1 \rangle \subseteq \langle y_1 \rangle$ and $\langle x_1 \rangle \subseteq I$. Now, consider the intersection $I \cap \langle y_1 \rangle$. We have that $\langle x_1 \rangle \subseteq (\langle y_1 \rangle \cap I)$. We wish to show that $(\langle y_1 \rangle \cap I)$ is a prime ideal. We recall that in a Dedekind domain an ideal is prime if and only if it is maximal. Also, R a Dedekind domain implies that there exist nonzero prime ideals $P_1, \ldots, P_r$ such that $(\langle y_1 \rangle \cap I) = \prod_{i=1}^{r} P_i$. Then, $I \supseteq (\langle y_1 \rangle \cap I) = \prod_{i=1}^{r} P_i$, and as we showed in class, in a Dedekind domain, $(\langle y_1 \rangle \cap I) \supseteq \prod_{i=1}^{r} P_i$ implies $(\langle y_1 \rangle \cap I) \supseteq P_i$ for some $i \in [r]$.

Now, recall that in a Dedekind domain every nonzero ideal can be factored uniquely into a product of nonzero prime ideals, up to reordering. So, $(\langle y_1 \rangle \cap I) = \prod_{i=1}^{s} Q_i$ and $(\langle y_1 \rangle \cap I) = \prod_{i=1}^{s} Q_i \supseteq P_i$. Now, as shown in class, $(\langle y_1 \rangle \cap I) = \prod_{i=1}^{s} Q_i \supseteq P_i$ implies that there exists an ideal C such that $P_i = C \prod_{i=1}^{s} Q_i = \prod_{i=1}^{t} W_i \prod_{i=1}^{s} Q_i = (\prod_{i=1}^{t} W_i)(\langle y_1 \rangle \cap I)$. In particular, this implies that $t + s = 1$, which means that $s = 1, t = 0$. (Otherwise, if $s = 0, t = 1$ then $\prod_{i=1}^{s} Q_i = (\langle y_1 \rangle \cap I) = R$ which implies that $I = R$, a contradiction since R is not a prime ideal by definition). So, $s = 1, t = 0$ and $Q_1 = P_i$. Finally, we get $(\langle y_1 \rangle \cap I) = \prod_{j=1}^{s} Q_j = P_i$. So, $(\langle y_1 \rangle \cap I)$ is prime and nonzero since $P_i \neq 0$ since $P_i = 0$ would imply that . Since any non zero prime ideal is maximal in a Dedekind domain, $(\langle y_1 \rangle \cap I)$ is maximal. Then, $(\langle y_1 \rangle \cap I) \subseteq I$ and $I \neq R$ implies that $I = (\langle y_1 \rangle \cap I)$. Then, $(\langle y_1 \rangle \cap I) \subseteq \langle y_1 \rangle$ and $\langle y_1 \rangle \neq R$ (Why? Since y_1 irreducible implies $\langle y_1 \rangle$ contains no units, which implies $\langle y_1 \rangle \neq R$. Why does it contain no units? Assume it did. Then, $y_1 x = u$ with u a unit, and then $y_1 x u^{-1} = 1$ but then y_1 is a unit, a contradiction, by definition of an irreducible element). So, $(\langle y_1 \rangle \cap I) \subseteq \langle y_1 \rangle$ and $\langle y_1 \rangle \neq R$ implies that $(\langle y_1 \rangle \cap I) = \langle y_1 \rangle$. So, we have $\langle y_1 \rangle = (\langle y_1 \rangle \cap I) = I$ or $\langle y_1 \rangle = I$ which means that I is principal and we're done.

So, that concludes the proof that in a Dedekind domain which is a UFD, every prime ideal is principal. $\square$

Now, it remains to show that non-prime ideals in R are principal. Well, take I an ideal in R. As shown in class, since R is a Dedekind domain, we can uniquely factor $I = \prod_{i=1}^{r} P_i$. Then, recall $P_i = \langle x_i \rangle$ by the lemma we just proved. So, $I = \prod_{i=1}^{r} \langle x_i \rangle = \langle \prod_{i=1}^{r} x_i \rangle$ and we see that I is generated by one element, which concludes this problem.

5

Take $\alpha_1 = 1$ and $\alpha_2 = 1+i$. Then, one notes that $\alpha_2 - \alpha_1 = i$ so that $Z[i] = Z + Zi = Z\alpha_1 + Z(\alpha_2 - \alpha_1) = Z\alpha_1 + Z\alpha_2 - Z\alpha_1 = \{a\alpha_1 + b\alpha_2 + (-c)\alpha_1 : a, b, c \in Z\} = \{a'\alpha_1 + b'\alpha_2 + : a', b' \in Z\}$. Why? Obviously, $\{a'\alpha_1 + b'\alpha_2 + : a', b' \in Z\} \subseteq \{a\alpha_1 + b\alpha_2 + (-c)\alpha_1 : a, b, c \in Z\}$ by taking $a := a'$, $b := b'$ and $c := 0$. Now for the reverse, we wish to show $\{a\alpha_1 + b\alpha_2 + (-c)\alpha_1 : a, b, c \in Z\} \subseteq \{a'\alpha_1 + b'\alpha_2 + : a', b' \in Z\}$. Namely, given a, b, c, we wish to produce $a', b' \in Z$ such that $a\alpha_1 + b\alpha_2 + (-c)\alpha_1 = a'\alpha_1 + b'\alpha_2 \in \{a'\alpha_1 + b'\alpha_2 + : a', b' \in Z\}$. Let $a' := a - c$ and $b' := b$. Then, we are done. So, $Z[i] = Z + Zi = Z\alpha_1 + Z(\alpha_2 - \alpha_1) = \{a'\alpha_1 + b'\alpha_2 + : a', b' \in Z\} = Z\alpha_1 + Z\alpha_2$.

Then, we note that $(1+i)Z[i] = (2\alpha_1)Z + \alpha_2 Z$. Why? $(1+i)Z[i] = \{(1+i)(a+bi) : a, b \in Z\}$. We wish to show that $(1+i)Z[i] = (2\alpha_1)Z + \alpha_2 Z$. We need to show $(1+i)Z[i] \subseteq (2\alpha_1)Z + \alpha_2 Z$ and $(2\alpha_1)Z + \alpha_2 Z \subseteq (1+i)Z[i]$. To show that $(1+i)Z[i] \subseteq (2\alpha_1)Z + \alpha_2 Z$, we need to show that for all $a, b \in Z$, there exists $r, s \in Z$ such that $(1+i)(a+bi) = r(2\alpha_1) + s(\alpha_2) = 2r + s(1+i)$. Note $(1+i)(a+bi) = (a-b) + (a+b)i = (2r+s) + si$ implies that $a + b = s$ and $a - b = 2r + s$ which implies that $2r = (a-b) - (a+b) = -2b$ so that $r = -b$. Then, $a - b = 2r + s = -2b + s$ implies that $a + b = s$. So, set $r := -b$ and $s := a + b$. For the reverse inclusion we need to show that $(2\alpha_1)Z + \alpha_2 Z \subseteq (1+i)Z[i]$. Namely, given any $r, s \in Z$, we wish to show that there exists $a, b \in Z$ such that $r(2\alpha_1) + s(\alpha_2) = 2r + s(1+i) = (1+i)(a+bi)$. Namely, one notes that as above this implies that $a - b = 2r + s$ and $a + b = s$. So, $2a = 2r + 2s$ or $a = r + s$ and $b = s - a = s - r - s = -r$. So, take $a = r + s$ and $b = -r$. Then, $(1+i)(a+bi) = a - b + (a+b)i = 2r + s + si = 2(r) + s(1+i) \in 2\alpha_1 Z + \alpha_2 Z$.

Then, $S_{(1+i)} = S \cup (S + \alpha_1)$.

Then, the relation to the norm is that $N_{Q(i)/Q}(1+i) = N((1+i)) = |O_K/(1+i)| = |Z[i]/(1+i)|$. Then, $Z[i]/(1+i) \cong Z\alpha_1 + Z\alpha_2/(Z2\alpha_1 + Z\alpha_2) \cong Z/2Z$ which means that $|Z[i]/(1+i)| = 2$.

6

Ok, $F = C(t)$ and $p(y) = y^2 - x(x-5)(x+5)$. Let $E := F[y]/(p(y))$ and $R := C[t]$. Say we denote the integral closure of R in E, namely the set of all elements $\alpha \in E$ such that $f(\alpha) = 0$ for some monic $f(x) \in R[x]$, by S. So,

$$S := \{\alpha \in E : f(\alpha) = 0 \text{ for some monic } f(x) \in R[x]\}.$$

We wish to show that $S = R[y]/(p(y))$. Say $\alpha \in F[y]/(p(y))$. We wish to construct $f \in R[x]$ monic such that $f(\alpha) = 0$.

THIS IS SCRATCH: Well, we know that there is some minimal polynomial of α over $F = C(t)$. Let it be

$$m_{\alpha/F}(x) = \sum_{i=0}^{N} \frac{a_i(t)}{b_i(t)} x^i$$

where $N \leq deg(p)$. Now, we know

$$m_{\alpha/F}(\alpha) = \sum_{i=0}^{N} \frac{a_i(t)}{b_i(t)} (\alpha)^i = 0$$

Pick some coset representative $a \in C(t)[y] = F[y]$ so that $\alpha = a + (p(y))$. Then,

$$\begin{aligned} m_{\alpha/F}(\alpha) &= \sum_{i=0}^{N} \frac{a_i(t)}{b_i(t)} (a(y) + (p(y)))^i = (p(y)) = 0 \in E \\ &= \big(\sum_{i=0}^{N} \frac{a_i(t)}{b_i(t)} (a(y))^i\big) + (p(y)) \end{aligned}$$

So, we wish to construct $g \in R[x]$ such that there is some coset representative $a' \in \alpha$ such that $g(a') = 0$. We let $B(t) = (lcm_{i \in \{0,\ldots,N\}}(b_i(t)))$ and $\hat{B}(t) = B(t)^N$ Then, define $B_i(t) = B^N(t)/b_i(t) = (B(t)/b_i(t))B^{N-1}(t)$ for all i. Note that $b_N(t) = 1$ so that $B_N(t) = B^N(t)$. Finally, note that for $i \in \{1, \ldots, n-1\}$ one has that $B_i(t) = (B(t)/b_i(t))B^{N-1-i}(t)B^i(t)$.

$$\begin{aligned} B^N(t) * m_{\alpha/F}(\alpha) &= \sum_{i=0}^{N} B_i(t)a_i(t)(a(y) + (p(y)))^i = B^N(t)(p(y)) = 0 \in E \\ &= \big(\sum_{i=0}^{N} B_i(t)a_i(t)(a(y))^i\big) + (p(y)) \\ &= B^N(t)(a(y))^N + \sum_{i=0}^{N-1} B_i(t)a_i(t)(a(y))^i + (p(y)) \\ &= (B(t)a(y))^N + \sum_{i=0}^{N-1} (a_i(t))(B(t)/b_i(t))B^{N-1-i}(t)B^i(t)a^i(y) + (p(y)) \\ &= (B(t)a(y))^N + \sum_{i=0}^{N-1} (a_i(t))(B(t)/b_i(t))B^{N-1-i}(t)(B(t)a(y))^i + (p(y)) \end{aligned}$$

Now, we wish to show that S is a dedekind domain. We need to show Noetherian, Height 1 and Integrally closed. Now, by the hint if one can show that C is noetherian, then $C[x]$ is noetherian, then $C[x][y]$ is noetherian. Then S is noetherian. So, I show that C is noetherian. This is simple. We need to show every ideal is finitely generated. However C a field implies that the only ideals are 0 and C. Then $0 = \langle 0 \rangle$ and $C = \langle 1 \rangle$. For height 1, we need to show that

For showing $S = R[y]/(p(y))$, say we have some prime ideal of S. Then, the inverse image of a nonzero prime ideal under a ring homomorphism is a nonzero prime ideal. So say $\phi : R = C[x] \to S$. Take a prime ideal $P \in S$. Then, we know that $\phi^{-1}(P) = P'$ a prime ideal $P' \leq R = C[x]$. Since C is a field, $C[x]$ is a PID, which means that elements are irreducible if and only if prime, so P' some ideal in this PID means it is generated by one element f which is irreducible so that $P' = \langle f \rangle$ and C algebraically closed means that the only irreducible polynomials are linear ones, so $f = x - a$ for some a in C. Then, just using ϕ the natural embedding of R into S. One notes that $\phi((x-a)) = P = \langle (x-a) + (p(y)) \rangle$. However, one then notes that if one picks $b \in E$ such that $b^2 = a(a-5)(a+5)$ then, $(y-b)(y+b) = y^2 - b^2 = y^2 - a(a-5)(a+5) \in (p(y))$ so that $P = \langle (x-a) + (p(y)) \rangle$. Then, the fact that $R[y]/(p(y))$ is an integral domain means that $(p(y))$ is a prime ideal. So, $y - b \in (p(y))$ or $y + b \in (p(y))$. Say $y - b \in (p(y))$. Then, $P = \langle (x-a) + (p(y)) \rangle = \langle (x-a) + (p(y)), (y-b) + (p(y)) \rangle$. Also, $b^2 = a(a-5)(a+5)$ implies that $(-b)^2 = a(a-5)(a+5)$. So, applying the same argument to $-b$ gives that $P = \langle (x-a) + (p(y)) \rangle = \langle (x-a) + (p(y)), (y+b) + (p(y)) \rangle$. So, $\phi^{-1}(\langle \langle (x-a) + (p(y)), (y+b) + (p(y)) \rangle \rangle) = \phi^{-1}(\langle \langle (x-a) + (p(y)), (y-b) + (p(y)) \rangle \rangle) = \langle x - a \rangle$.

Then, the integral closure of a set R in E is always integrally closed in E. So, S is integrally closed.

https://proofwiki.org/wiki/Transitivity_of_Integrality https://proofwiki.org/wiki/Integral_Closure_is_Integrally_Closed