

Solution 1.

Let $A \subseteq B$ be an integral extension of Dedekind domains, and let \mathfrak{p} be a prime ideal in A . Let $x \in \mathfrak{p} \setminus \mathfrak{p}^2$, (clearly as we are in A , a Dedekind domain, $\mathfrak{p} \setminus \mathfrak{p}^2$ is non-empty, also note that we have $x \neq 0$). Now $(x)\mathfrak{p}^{-1} \subseteq A$, furthermore, $(x)\mathfrak{p}^{-1} \not\subseteq \mathfrak{p}$ as otherwise $x \in \mathfrak{p}^2$. Thus, we may pick $\alpha \in (x)\mathfrak{p}^{-1}$ such that $\alpha \notin \mathfrak{p}$. We then have

$$(\alpha) \subseteq (x)\mathfrak{p}^{-1}$$

which implies

$$(\alpha)\mathfrak{p} \subseteq (x)$$

and consequently if $\mathfrak{p}B = B$ then

$$(\alpha)\mathfrak{p}B = (\alpha)B \subseteq (x)B$$

so $\alpha = xy$, for some $y \in B$, working in $\text{Frac}(B)$ we see that $y = \frac{\alpha}{x}$, hence $y \in \text{Frac}(A)$ and thus $y \in B \cap \text{Frac}(A) = A$ (clearly $A \subseteq B \cap \text{Frac}(A)$, conversely any element in $B \cap \text{Frac}(A)$ is integral over A and in the field of fractions of A so it must be in A as A is Dedekind, thus $B \cap \text{Frac}(A) \subseteq A$) and we thus have that $(\alpha) \subseteq (x) \subseteq \mathfrak{p}$ which contradicts our choice of α .

Alternate proof: Recall that Nakayama's lemma states that, if A is a commutative ring with unity, B a finitely generated A -module and I is an ideal of A such that $IB = B$, then there is an element $r \in I$ such that $(1 - r)B = 0$. (cf: Commutative Ring Theory by Matsumura)

As $A \subseteq B$ is an integral extension, we have that B is finitely generated as an A -module. If $\mathfrak{p}B = B$, we apply Nakayama's lemma to get some $r \in \mathfrak{p}$ such that $(1 - r)B = 0$, but as B is an integral domain we have that $1 - r = 0$ which gives that $r = 1$. But as $r \in \mathfrak{p}$ this implies that $\mathfrak{p} = A$, a contradiction. \square

Solution 2.

$K = \mathbb{Q}(\sqrt{-63}) = \mathbb{Q}(\sqrt{9}\sqrt{-7}) = \mathbb{Q}(\sqrt{-7})$, then as $-7 \equiv 1 \pmod{4}$ we have that $O_K = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ and $\text{Disc}(O_K) = -7$. Thus (by Theorem 3.37, Milne), 7 is the only prime that ramifies in O_K .

If $K = \mathbb{Q}(\sqrt{-57})$, then as $-57 \not\equiv 1 \pmod{4}$ we have that $O_K = \mathbb{Z}[\sqrt{-57}]$ and $\text{Disc}(O_K) = -4(57) = -(2)^2(3)(19)$. Thus (by Theorem 3.37, Milne), 2, 3 and 19 are the only primes that ramify in O_K . \square

Solution 3.

Let $\theta = 10^{\frac{1}{3}}$ and $K = \mathbb{Q}(\theta)$. Let O_K denote the ring of integers of the number field K . So $\mathbb{Z} \subseteq \mathbb{Z}[\theta] \subseteq O_K$. Now $\text{Disc}(\mathbb{Z}[\theta]) = -2700 = -(2)^2(3)^3(5)^2$. Thus, the only primes that may possibly ramify in O_K are 2, 3, 5, indeed as $\mathbb{Z}[\theta]$ has rank 4 (which is equal to the rank of O_K , as \mathbb{Z} -modules of course) we have that $[O_K : \mathbb{Z}[\theta]]$ is finite

and we thus know that $Disc(\mathbb{Z}[\theta]) = Disc(O_K) \cdot [O_K : \mathbb{Z}[\theta]]^2$, in particular $Disc(O_K)$ divides $Disc(\mathbb{Z}[\theta])$. From this it is also clear that 3 must ramify (as 3 occurs to an odd power in $Disc(\mathbb{Z}[\theta])$). Furthermore $(2, \theta)^3 = (8, 4\theta, 2\theta^2, \theta^3) = (8, 4\theta, 2\theta^2, 10) = (8, 4\theta, 2\theta^2, 10, 10 - 8) = (8, 4\theta, 2\theta^2, 10, 2) = (2)$. From this we have that $(2, \theta) \neq O_K$, (as otherwise $1 \in (2, \theta)^3 = (2)$ and $2O_K = O_K$ which can't happen by problem 1), and any prime ideal that divides $(2, \theta)$ in O_K also divides (2) with multiplicity 3, thus 2 must ramify. Similarly, $(5, \theta)^3 = (125, 25\theta, 5\theta^2, \theta^3) = (125, 25\theta, 5\theta^2, 10) = (125, 25\theta, 5\theta^2, 10, 125 - 10 \cdot 10) = (125, 25\theta, 5\theta^2, 10, 5) = (5)$, so 5 must also ramify. \square

Solution 4.

Let $\theta = 10^{\frac{1}{3}}$, $K = \mathbb{Q}(\theta)$ and O_K the ring of integers of K . By the previous problem we know that 2, 3 and 5 are the only primes that ramify in O_K thus these are the only primes that occur in the factorization of $Disc(O_K)$. Let $\alpha = \frac{1+\theta+\theta^2}{3}$, clearly $\alpha \in K$, furthermore α is a root of $x^3 - x^2 - 3x - 3$, and thus $\alpha \in O_K$. But $Disc(\mathbb{Z}[\alpha]) = -300 = -(2)^2(3)(5)^2$, thus $Disc(O_K)$ divides -300 (as $\mathbb{Z}[\alpha]$ has finite index in O_K , cf. Remark 2.24 in Milne). But from the previous problem we know that 2, 3, 5 ramify in O_K and must thus divide $Disc(O_K)$, consequently, (as $Disc(\mathbb{Z}[\alpha]) = Disc(O_K) \cdot [O_K : \mathbb{Z}[\alpha]]^2$), we have that $Disc(O_K) = -300$ and $[O_K : \mathbb{Z}[\alpha]] = 1$ or $O_K = \mathbb{Z}[\alpha]$.

Now using Maple we have that

$$\begin{aligned} X^3 - X^2 - 3X - 3 \pmod{2} &= (X + 1)^3 \\ X^3 - X^2 - 3X - 3 \pmod{3} &= (X)^2(X + 2) \\ X^3 - X^2 - 3X - 3 \pmod{7} &= (X^3 - X^2 - 3X - 3) \\ X^3 - X^2 - 3X - 3 \pmod{11} &= (X^2 + 3X + 9)(X + 7) \\ X^3 - X^2 - 3X - 3 \pmod{37} &= (X + 8)(X + 10)(X + 18) \end{aligned}$$

Thus, by Theorem 3.43 in Milne we have the following factorizations

$$\begin{aligned} 2O_K &= (2, \alpha + 1)^3 \\ 3O_K &= (3, \alpha)^2(3, \alpha + 2) \\ 7O_K &= (7, \alpha^3 - \alpha^2 - 3\alpha - 3) = (7, 0) = (7) \\ 11O_K &= (11, \alpha^2 + 3\alpha + 9)(11, \alpha + 7) \\ 37O_K &= (37, \alpha + 8)(37, \alpha + 10)(37, \alpha + 18) \end{aligned}$$

\square

Solution 5.

Let $K = \mathbb{Q}(i, \sqrt{5})$, O_K the ring of integers of K , $L = \mathbb{Q}(\sqrt{-5})$ and O_L the ring of integers of O_L . Note that $O_L = \mathbb{Z}[\sqrt{-5}]$ and $Disc(O_L) = -20 = -(2)^2(5)$. Thus 2, 5 ramify in O_L . But clearly as $L \subseteq K$ we have that $O_L \subseteq O_K$ so 2, 5 ramify in O_K (by the same reasoning as used in problem 3), we claim that 2, 5 are the only primes that ramify in O_K .

Let $R = \mathbb{Z}[i, \sqrt{5}, i\sqrt{5}]$. Clearly $\mathbb{Z} \subseteq R \subseteq O_K$. Now

$$Disc(R) = \begin{vmatrix} 1 & i & i\sqrt{5} & \sqrt{5} \\ 1 & -i & -i\sqrt{5} & \sqrt{5} \\ 1 & i & -i\sqrt{5} & -\sqrt{5} \\ 1 & -i & i\sqrt{5} & -\sqrt{5} \end{vmatrix}^2 = (2)^8(5)^2$$

Now as R is of finite index in O_K we have that $Disc(O_K)$ divides $Disc(R)$ and thus we know that the only primes that may ramify in O_K are 2, 5. We have already shown that they both do and thus we are done. \square