Answers to the problem set 6 [1]

Exercise 6.1: If A is a Dedekind domain and L is a finite separable extension of $\mathrm{Frac}(A)$, then the integral closure of A in L is also a Dedekind domain. So, since $\mathbb{Z}$ is Dedekind, then so is O_K. Now, if p is a prime ideal of $\mathbb{Z}$, then we know there is at least one prime above p in O_K. Hence, since there are infinitely many primes in $\mathbb{Z}$, so in O_K.

Exercise 6.2: 1) $S^{-1}B = L$ exactly means for any $l \in L$ there exists $a \in A\backslash\{0\}$ such that $al \in B$. But since L is algebraic over K there exist $a_0, \cdots, a_n \in K$ s.t. $l^n + l^{n-1}a_{n-1} + \cdots + a_0 = 0$. But, since $K = \mathrm{Frac}(A)$ there exists $d \in A$ such that $da_i \in A$. Now we have:

$$(dl)^n + (dl)^{n-1}(da_{n-1}) + \cdots + d^n a_0 = 0$$

So dl is integral over A and hence $dl \in B$.

2) If $K \subseteq L$ is any field extension then $\alpha \in L$ is algebraic over K iff $K[\alpha] = K(\alpha)$. Now we know there exists $\alpha \in L$ such that $L = K(\alpha)$. But, because of (1) there exists $d \in A$ such that $d\alpha \in B$. But since $d \in K$ obviously $K(d\alpha) = K(\alpha)$. So, $K(d\alpha) = K[d\alpha] = L$ and $d\alpha \in B$.

3) If $g \in A[x]$ is a monic polynomial which $g(\alpha) = 0$ and f is the minimal polynomial of α over K and β is another root of f, since $f|g$ then β is also a root of g. So, roots of f are all integral over A and therefore $f \in A[x]$.

4) Define $\phi : A[x] \to B$, then because of (3) $\mathrm{Ker}(\phi) = (f(x))$. Hence (4).

5) Let discuss this problem at the tutorial.

Exercise 6.3: 1) No! Since if ω is the third root of unity then $\omega\sqrt[3]{2}$ must lie inside the Galois closure of $\mathbb{Q}(\sqrt[3]{2})$and hence $\omega = \omega\sqrt[3]{2}/\sqrt[3]{2}$. But, the minimal polynomial of ω has degree 2 over $\mathbb{Q}$. So 2 would divide the degree of the Galois closure of $\mathbb{Q}(\sqrt[3]{2})$. Therfore since the degree of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ is 3, we are done.

2,3) Since $O_K = \mathbb{Z}[\sqrt[3]{2}]$, we can use exercise 6.2.5. Here $f(x) = x^3 - 2$ and $p = 3$. But, $x^3 - 2 = (x+1)^3$. Hence $g = 1, e = 3, f = 1$.

Exercise 6.4: We assume m is odd.

1) It is just the known formula $\sum e_i f_i = n$. Here n is 2, so g is at most 2.

2) First, we show that pA cannot be of the form $\mathfrak{p}^2$ where $\mathfrak{p}$ is a prime ideal in O_K, $K = \mathbb{Q}(\sqrt{m})$. This would prove (b) by (a). Assume $pA = \mathfrak{p}^2$. Then $\mathfrak{p} \nsubseteq pA$, so we can find $x = a + b\sqrt{m}$ where p does not divide neither a nor b. Note that if for instance p divides a then $p|b\sqrt{m} \Rightarrow p|b^2m \Rightarrow p|b$. Now, take the $\mathbb{Q}-$automorphism $\sigma : \mathbb{Q}(\sqrt{m}) \to \mathbb{Q}(\sqrt{m})$ which sends $\sqrt{m}$ to $-\sqrt{m}$. Since σ maps the prime ideals pA in O_K since, obviously, sends O_K to O_K. So we have $pA = \sigma(pA) = \sigma(\mathfrak{p})^2$. σ is an automorphism so it maps the prime ideals of O_K to themselves, hence we have $\sigma(\mathfrak{p}) = \mathfrak{p}$. Therefore, $\sigma(x) = a - b\sqrt{m} \in \mathfrak{p}$. Now, $x + \sigma(x) = 2a - \in pA$. Hence, $p|2a \Rightarrow p|a$, contradiction!

If $pA = \mathfrak{p}_1\mathfrak{p}_2$ then as above $\sigma(\mathfrak{p}_1)$ must be $\mathfrak{p}_2$. Now, since none of $\mathfrak{p}_i$'s lies inside pA, we can take $x \in \mathfrak{p}_1\backslash pA$. Hence $x.\sigma(x) = a^2 - b^2m \in \mathfrak{p}_1\mathfrak{p}_2 \Rightarrow p|a^2 - b^2m \Rightarrow (\frac{a}{b})^2 \equiv m \pmod{p}$.

[1] Questions and comments to siinarezazadeh@gmail.com or come to office A3, 111.

Conversely, if $a^2 \equiv m \pmod{p}$ then both $a - \sqrt{m}$ and $a + \sqrt{m}$ cannot lie inside the same prime above p in O_K. Since, otherwise, as above, p would divide a. So, there are at least two primes above p. So, we are done.

3) For the case $p = 2$ go to (4), so we assume p is odd and divides m. As we know from the previous exercises $O_K = \mathbb{Z}[\sqrt{m}]$ when $m \equiv 2, 3 \pmod{4}$. So, if we use 6.2.5 we will see p ramifies since $x^2 - m = x^2 \pmod{p}$ in $\mathbb{Z}[X]$, note that here we just need p to divide m. Now if $m \equiv 1 \pmod{4}$ then $O_K = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ and $f(X) = X^2 - X + \frac{1-m}{4}$ would be the minimal polynomial of $\frac{1+\sqrt{m}}{2}$. But this way, $\bar{f}(X) = \overline{(X - \frac{1}{2})}^2$, note that since p is odd $\frac{1}{2} \in \mathbb{F}_p^*$ makes sense.

4) If $p = 2$ and $m \equiv 1 \pmod{4}$ then if $f(X) = \bar{X}^2 - \bar{X} + \frac{1-m}{4}$ we would have $\bar{f}(X) = X^2 - X \in \mathbb{F}_2[X]$ whenever $m \equiv 1 \pmod{8}$ and $\bar{f}(X) = X^2 - X + 1 \in \mathbb{F}_2[x]$ in the case $m \equiv 5 \pmod{8}$. So, we have 4).