1. Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{7})$. Find the degree of the extension $K/\mathbb{Q}$. That is, compute $[K : \mathbb{Q}]$.

Solution Start with finding the primitive element of the field K. The primitive element theorem dictates that any number field must have a primitive element. We claim that the primitive element is $\sqrt{7}+\sqrt{3}$. We wish to show $\mathbb{Q}(\sqrt{3}, \sqrt{7}) = \mathbb{Q}(\sqrt{3}+\sqrt{7})$. It suffices to show that each of the generators are included in the other field. We prove the following to relations:

$$\sqrt{7}+\sqrt{3} \in \mathbb{Q}(\sqrt{7}, \sqrt{3}) \quad \text{and} \quad \sqrt{7}, \sqrt{3} \in \mathbb{Q}(\sqrt{7}+\sqrt{3})$$

The first statement follows trivially from the additive closure of the field $\mathbb{Q}(\sqrt{7}, \sqrt{3})$. For the second statement, exploit the existance of multiplicative inverses. We know that the following element exists in $\mathbb{Q}(\sqrt{7}+\sqrt{3})$.

$$4 \cdot (\sqrt{7}+\sqrt{3})^{-1} = \frac{4}{\sqrt{7}+\sqrt{3}} = \frac{4(\sqrt{7}-\sqrt{3})}{(\sqrt{7}+\sqrt{3})(\sqrt{7}-\sqrt{3})} = \sqrt{7}-\sqrt{3}$$

We have obtained that the sum and difference of $\sqrt{3}, \sqrt{7}$ are both in the field $\mathbb{Q}(\sqrt{7}, \sqrt{3})$. Thus,

$$\frac{(\sqrt{7}+\sqrt{3})+(\sqrt{7}-\sqrt{3})}{2} = \sqrt{7} \in \mathbb{Q}(\sqrt{7}, \sqrt{3})$$
$$\sqrt{7}-(\sqrt{7}-\sqrt{3}) = \sqrt{3} \in \mathbb{Q}(\sqrt{7}, \sqrt{3})$$

Thus, $K = \mathbb{Q}(\sqrt{7}+\sqrt{3})$. The degreee of the extension $K/\mathbb{Q}$ equals to the minimum polynomial of the generator. In search for a minimum polynomil, we first observe some relations around the generator. For convinience, let $\theta := \sqrt{7}+\sqrt{3}$. We have shown above that:

$$4/\theta = \sqrt{7}-\sqrt{3} = \theta - 2\sqrt{3}$$

$$\theta - 4/\theta = 2\sqrt{3} \quad \text{and} \quad (\theta - 4/\theta)^2 = 12$$
$$\theta^2 - 8 + 16/\theta^2 = 6$$
$$\theta^4 - 20\theta^2 + 16 = 0$$

We purport that the polynomial $\theta^4 - 20\theta^2 + 16$ is irrecucible in $\mathbb{Z}$. Apply the mod 5 test to show that the equation has no linear factors. Assuming the polynomial has at least one lienar factor, the following must hold:

$$\theta^4 + 1 \equiv 0 \mod 5 \quad \text{or} \quad \theta^4 \equiv -1 \mod 5$$

With some basic arithmetic, we verify that -1 is not a quintic residue of 5. Hence there are no linear factors.

For the quintic polynomial has no lienar factors, it must factor into two quadratic polynomials assuming it is reducible. We write:

$$(\theta^2 + a\theta + b)(\theta^2 - a\theta + c) = \theta^4 - 20\theta^2 + 16$$

where $a, b, c \in \mathbb{Z}$

The coefficient of θ of the two linear factors must differ by a factor of -1 for their product to have no terms of θ^3. Furthermore, comparing the coefficient of θ, we observe $ac - ab = a(c - b) = 0$. Either $a = 0$ or $c - b = 0$. If $a = 0$, applying the substitution $x := \theta^2$, we write:

$$(x + b)(x + c) = x^2 - 20x + 16$$

By the quadratic formula, $b = 10 \pm \sqrt{84}$. But then, $b \notin \mathbb{Z}$. This is a contradiction.

We revert to the only alternative $c - b = 0$ or $c = b$.

$$(\theta^2+a\theta+b)(\theta^2-a\theta+b) = (\theta^2+b+a\theta)(\theta^2+b-a\theta) = (\theta^2+b)^2-a^2\theta^2 = \theta^4-20\theta^2+16$$

So $b^2 = 16$ and $b = \pm 4$. $2b - a^2 = -20$ so either $8 - a^2 = -20$ or $-8 - a^2 = -20$. a^2 must either be 28 or 12. In both cases, a is not an integer. The polynomial must be irreducible.

Thus:

$$[K : Q] = 4$$

□

2. Find all integer solutions to the equation $x^2 + 13 = y^3$.

Solution We begin with some divisibility relations of x, y in $\mathbb{Z}$. $13 \nmid x$ and y must be odd. To show $13 \nmid x$, assume $13|x$. From $x^2 + 13 = y^3$, we observe that 13 divides the LHS so it must also divide the RHS, hence $13|y$. However, 13 divides the LHS exactly once while it divides the RHS thrice. We reach a contradiction and conclude $13 \nmid x$.

It is possible to show y odd in a similar manner. Assume y to be even. x must be odd.

$$y^3 \equiv 0 \mod 4$$

but

$$x^2 + 13 \equiv 1 \quad \text{or} \quad 2 \mod 4$$

so

$$x^2 + 13 \not\equiv y^3 \mod 4$$

and y must be odd.

Factor the equation in the ring of integers of the field $\mathbb{Q}(\sqrt{-13})$.

$$(x - \sqrt{-13})(x + \sqrt{-13}) = y^3$$

Passing up to the ideals:

$$\langle x - \sqrt{-13}\rangle\langle x + \sqrt{-13}\rangle = \langle y\rangle^3$$

The two ideals are coprime. Assume for a contradiction that some prime ideal $\mathfrak{p}$ divides both ideals. Division implies inclusion, so we write:

$$\langle x - \sqrt{-13}\rangle, \langle x + \sqrt{-13}\rangle \subseteq \mathfrak{p} \quad \text{and} \quad x \pm \sqrt{-13} \in \mathfrak{p}$$

Thus:

$$2x, 2\sqrt{-13} \in \mathfrak{p}$$

By strong closure of ideals, we deduce that $-2\sqrt{-13}^2 = 26$ is an element of $\mathfrak{p}$. Since $13 \nmid x$,

$$\gcd(2x, 26) = 2 \quad \text{and} \quad (2x)s + 26t = 2$$

where the latter equation obtained from Bezouts identity. s, t are integers. We write $2 \in \mathfrak{p}$.

Moreover, $\mathfrak{p}|\langle y\rangle^3$ and thus $\mathfrak{p}|\langle y\rangle$ and $y \in \mathfrak{p}$. We have shown previously that y is odd. Thus, $y - 2v = 1$ for some integer v. This implies $1 \in \mathfrak{p}$ and $\mathfrak{p} = \mathcal{O}_K$, a contradiction. ↯

Ideals factor uniquely into prime ideals in any Dedekind Domain. Recall the equation:

$$\langle x - \sqrt{-13}\rangle\langle x + \sqrt{-13}\rangle = \langle y\rangle^3$$

Where the two ideals on the left are coprime. It must be:

$$\langle x - \sqrt{-13}\rangle = I^3$$

for some ideal I. In light of the class group, the left ideal is principal so it belongs to the principal ideal group. I^3 must also belong to the principal class. We know that the class number of $\mathbb{Q}(\sqrt{-13})$ is 2. If I is not in the principal class, so will I^3 not be in the principal class. Hence, I must be principal.

$-13 \equiv 3 \mod 4$ so the integers of this field are in the form of $a + b\sqrt{-13}$ for integers a, b. The generator must I must also be an integer in the field $\mathbb{Q}(\sqrt{-13})$. Write:

$$\langle x - \sqrt{-13} \rangle = \langle a + b\sqrt{-13} \rangle^3 = \langle (a + b\sqrt{-13})^3 \rangle$$

The generators of a principal ideal must differ by a factor of a unit. We know that the only units of an imaginary quadriatic field is ± 1. So:

$$x - \sqrt{-13} = \pm(a + b\sqrt{-13})^3 = \pm\Big([a^3 - 39ab^2] + \sqrt{-13}[3a^2b - 13b^2] \Big)$$

Comparing the coefficient of $\sqrt{-13}$:

$$3a^2 - 13b^3 = \pm 1$$

b divides the LHS so it must divide the RHS. Thus, $b = \pm 1$. Plugging, in, we obtain $3a^2 - 13 = \pm 1$ or $3a^2 = 13 \pm 1$. The only integer solutions to the equation are $a = \pm 2$. Comparing the integer coefficient of the generator equation:

$$x = \pm(a^3 - 39ab^2) = \pm a(a^2 - 39) = \pm 70$$

Each of $x = \pm 70$ both yield $y = 17$. There exists no other solution.

$$\boxed{(x, y) = (\pm 70, 17)}$$

3. Prove that if a prime number p is totally ramified in a field K and not ramified in the field L, then $K \cap L = \mathbb{Q}$.

Proof Note that the field $M := K \cap L$ is a field extension of $\mathbb{Q}$. Take any two elements $a, b \in M$. $a - b \in K, L$ for K, L are both fields. $a - b \in K \cap L = M$. The multiplicative closure and existance of inverses can be shown in a similar fashion. $\mathbb{Q} \subseteq K$ and $\mathbb{Q} \subseteq L$ so $\mathbb{Q} \in L$.

For p is unramified in the extension L, it cannot be ramified in the smaller field M. We conclude that in the ring $\mathcal{O}_M$, $\langle p \rangle \mathbb{Z}$ is a prime ideal.

Write out the inertial degree of prime p over the ideal $\mathfrak{p} \in \mathcal{O}_K$. By the multiplicativity of the inertial degree:

Note that $\mathfrak{p} \cap \mathcal{O}_M$ is a prime ideal, for the intersect of a prime ideal in a smaller ring is also a prime ideal. If the intersect is not a prime ideal, two elements outside the prime ideal will multiply to be included in the prime ideal, and the same two elements will contradict the primeness of the larger ideal, leading to a contradiction.

Also, $\mathfrak{p}|\mathfrak{p}^n$ so $\mathfrak{p}|\langle p\rangle\mathbb{Z}$ meaning $p \in \mathfrak{p}$. Thus, $\langle p\rangle\mathbb{Z} \subseteq \mathfrak{p}$, and $\langle p\rangle\mathbb{Z} \subseteq \mathcal{O}_M$. Hence, $\langle p\rangle\mathbb{Z} \subseteq \mathfrak{p} \cap \mathcal{O}_M$. Inclusion implies division for ideals in Dedikind domains, so $\langle p\rangle\mathbb{Z}|\mathfrak{p} \cap \mathcal{O}_M$. The latter ideal is assumed to be prime, and we have previously shown that the principal ideal generated by p is prime in the ring $\mathcal{O}_M$. The two ideals must equal to each other, or in symbols:

$$\mathfrak{p} \cap \mathcal{O}_M = \langle p\rangle\mathbb{Z}$$

Since p is unramified in M, we write:

$$f(\mathfrak{p} \cap \mathcal{O}_M|p) = 1 \quad \text{or} \quad [\mathcal{O}_M/p\mathbb{Z} : \mathbb{Z}/p\mathbb{Z}] = 1$$

It must be $\mathcal{O}_M = \mathbb{Z}$ which in turn implies $M = \mathbb{Q}$. □

4. Let $K := \mathbb{Q}(\theta)$ where θ is a root of the polynomial $t^3 + t + 1$.

i) Prove that $\mathcal{O}_K = \mathbb{Z}[\theta]$. We claim that the set $\{1, \theta, \theta^2\}$ is an integral basis of the field K. Theorem 2.17 of the book states that if the discriminant of a field is squarefree, the $\mathbb{Q}$ basis of K must be an integral basis of $\mathcal{O}_K$. We know that the set $\{1, \theta, \theta^2\}$ is a $\mathbb{Q}$ basis of the field K. Also, from HW4, we have derived a formula for discirminants of cubic fields.

The discriminant of the power basis in the field $\mathbb{Q}(\theta)$ where θ where θ is a root of $t^3 + at + b$ is:

$$\Delta[1, \theta, \theta^2] = -4a^3 - 27b$$

So for the field K, the discriminant is:

$$\Delta[1, \theta, \theta^2] = -4 - 27 = -31$$

And this value is squarefree. By theorem 2.17, we conclude that the power set is indeed a integral basis. The $\mathbb{Z}$ span of the set $\{1, \theta, \theta^2\}$ is the set $\mathbb{Z}[\theta]$. Thus, $\mathcal{O}_K = \mathbb{Z}[\theta]$. □

ii) provide all the possible decomposition of the principal ideal generated by p.

Solution The integers of K are elements of $\mathbb{Z}[\theta]$. Theorem 10.1 of the textbook dictates exactly how the prime ideal $\langle p\rangle$ must decompose. Say that minimum polynomial of θ, which is $t^3 + t + 1$, factorize into some product of irreducible $\mathbb{Z}_p$ polynomials. Write:

$$t^3 + t + 1 = \prod_{i=1}^{n} f_i(t)^{e_i}$$

where $n \leq 3$ and all $f_i(t) \in \mathbb{Z}_p[t]$ are irreducible. Then we know that the factorization of $\langle p\rangle$ is given as:

$$\langle p\rangle = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i} \quad \text{where} \quad \mathfrak{p}_i = \langle p, f_i(i)\rangle$$

We observe that t^2+t+1 is irreducible in $\mathbb{Z}_2$. This can be easily shown by the mod 2 test. The cubic has no linear factors, and hence is irrecucible. Also, $t^2+t+1=(t^2+t+2)(t-1)$ in $\mathbb{Z}_3$, and the factors are all irredicible. Irreducibility of each terms can also easily be computed by the mod 3 test.

By Theroem 10.1, write:

$$\langle 2\rangle \text{ Prime} \quad \text{and} \quad \langle 3\rangle = \langle 3, \theta-1\rangle\langle 3, \theta^2+\theta+2\rangle$$

These two examples show that ideal $\langle p\rangle$ can either be a prime ideal or factor into two distinct prime ideals. The distinctness also comes from Theorem 10.1.

It can be easily demonstrated that $\langle p\rangle$ cannot be decomposed into a square of some prime ideal. Assume for a contradiction:

$$\mathfrak{p}^2 = \langle p\rangle$$

Then by taking the norm both sides:

$$N(\mathfrak{p}^2) = N(\langle p\rangle) = p^3$$

since $[K:Q]=3$. Let v denote $N(\mathfrak{p})$. We obtain $v^2=p^3$ for integer v. p is prime and no integer solutions exists, hence a contradiction. $\lightning$

We assume that $\langle p\rangle$ can decompose into some three distinct prime ideals.

Consider the case that $\langle p\rangle$ decomposes into $\mathfrak{p}_1^2\mathfrak{p}$. By Theorem 10.1, t^3+t+1 must factorize in the form of $(t-a)^2(t-b)$ over $\mathbb{Z}_p$. Write:

$$(t-a)^2(t-b) = t^3+t+1 \quad \text{poly mod}p$$

$$x^3-(2a+b)x+a^2+2ab-a^2b = t^3+t+1 \quad \text{poly mod}p$$

Comparing coefficients:

$$2a+b=0 \quad \text{and} \quad a^2+2ab=1 \quad \text{and} \quad -a^2b=-1 \mod p$$

So $b=-2a$ and $a^2-4a^2=1$ or $-3a^2=1$ or $(-3)a^2=1$. $a^2b=1$ and $\mathbb{Z}_p$ is a field so the mutiplicative inverse of a^2 must be unique. $b=-3$ and $a=-b2^{-1}=3(p+1)/2$. It is safe to assume p odd, for we have already ruled out the case $p=2$.

Plugging in $a=3(p+1)/2$, $b=-3$ to a^b yields $p=31$. We conclude:

$$(t-17)^2(t+3) = t^3+t+1 \quad \text{poly mod}31$$

Thus:

$$\langle 31\rangle = \langle 31, \theta+17\rangle^2\langle 31, \theta-3\rangle$$

It is impossible for $\langle p\rangle$ to completely ramify in K. If so, again by Thm 10.1, we obtain:

$$(t-n)^3 = t^3+t+1 \quad \text{poly mod}p$$

And by comparing coefficients, $3n = 0$, $3n^2 = 1$, $n^3 = 1$ mod p. $(3n)n = (0)n = 1$ so $0 = 1$ mod p, and we reach a contradiction.

To summarize, all possible decomposition of $\langle p \rangle$ in K are:

$$\langle p \rangle = \mathfrak{p} \quad \text{or} \quad \mathfrak{p}_1\mathfrak{p}_2 \quad \text{or} \quad \mathfrak{p}_1^2\mathfrak{p}_2 \quad \text{or} \quad \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$$

□

5. Let K be any number field and $\mathcal{O}_K$ be the ring of integers. Prove the following:

i) If π is irreducible in $\mathcal{O}_K$ and $\langle \pi \rangle$ is not a prime ideal, then $\langle \pi \rangle$ is not contained in any prime ideal.

Proof Assume for a contradiction, that π is irreducible and $\langle \pi \rangle$ is not prime but there exists a prime principal ideal $\langle a \rangle$ that includes $\langle \pi \rangle$. Inclusion implies division for ideals in a Dedekind domain. Hence:

$$\langle a \rangle | \langle \pi \rangle \quad \text{and} \quad \langle \pi \rangle = I\langle a \rangle$$

for some ideal I. Passing the equation up to the class group:

$$[\langle \pi \rangle] = [I][\langle a \rangle] \quad \text{and} \quad [I] = [\langle 1 \rangle]$$

So I must be principal. Let $I := \langle b \rangle$. We have $\langle \pi \rangle = \langle b \rangle\langle a \rangle = \langle ba \rangle$. The generators of the same principal ideal must differ by a unit. For some unit μ:

$$\pi = \mu ab$$

And we are given that π is irreducible. Necessarily, a or b must be a unit. If a is a unit, $\langle a \rangle$ will not be a proper principal ideal. If b is a unit, $\langle pi \rangle = \langle a \rangle$ and $\langle \pi \rangle$ will be prime. ↯ □

ii) Suppose $h_k = 2$. π is irreducible in $\mathcal{O}_K$ and $\langle \pi \rangle$ is not a prime ideal. Prove that $\langle p \rangle$ decomposes into two not necessarily distinct ideals.

Proof Decompose the ideal $\langle \pi \rangle$ into a product of prime ideals.

$$\langle \pi \rangle = \prod_{i=1}^{t} \mathfrak{p}_i^{e_i}$$

By part i), we deduce that none of $\mathfrak{p}_i$ can be principal. All of the prime ideals are in the same class group; the non-principal group. However, the product of all the prime ideals up to multiplicity, form a principal ideal. Relabeling the factors, write:

$$\langle \pi \rangle = \prod_{i=1}^{t} \mathfrak{p}_i\mathfrak{q}_i = \prod_{i=1}^{t} \langle \alpha_i \rangle = \left\langle \prod_{i=1}^{t} \alpha_i \right\rangle$$

where $\mathfrak{p}_i\mathfrak{q}_i = \langle \alpha_i \rangle$. For π is irreducible, without loss of generality, α_1 is an associate of π, and all other α_i's are units. For $i > 1$, by assumption, $\mathfrak{p}_i\mathfrak{q}_i =$

$\langle \alpha_i \rangle = \mathcal{O}_K$. This implies $\mathfrak{p} | \mathcal{O}_K$, a contradiction. Thus, the product simplifies to the first pair of which α_1 is an associate of π. In symbols:

$$\langle \pi \rangle = \mathfrak{p}\mathfrak{q}$$

□

Remark It follows that two ideals $\mathfrak{p}, \mathfrak{q}$ are both non-principal.

iii) Prove that if $h_k = 2$, then the factorization of any element has the same number of irreducibles.

Proof

Assume for a contradiction that there exists some element that has two factorizations that have different number of irreducibles associated with itself. Let α be an element in $\mathcal{O}_K$ be such an element with minimum number of irreducibles in its shortest factorization. Write:

$$\alpha = \beta_1 \beta_2 \cdots \beta_n = \gamma_1 \gamma_2 \cdots \gamma_m$$

where the beta-factorization is the shortest factorization (meaning least irreducible factors) of α, so $n < m$. None of the beta-gamma pairs can be associates. Ohterwise, by cancellation, we obtain an element with a shorter minimal factorization.

Passing the equation to ideals:

$$\langle \alpha \rangle = \langle \beta_1 \rangle \langle \beta_2 \rangle \cdots \langle \beta_n \rangle = \langle \gamma_1 \rangle \langle \gamma_2 \rangle \cdots \langle \gamma_m \rangle$$

We claim that none of the principal ideals generated by betas or gammas are prime. Assume for a contradiction, WLOG, that $\langle \beta_1 \rangle$ was prime. Ideals factor uniquely, so WLOG $\langle \beta_1 \rangle | \langle \gamma_1 \rangle$. If $\langle \gamma_1 \rangle$ is not prime, we reach a contradiction from part i). So $\langle \gamma_1 \rangle$ is prime and it must be equal to $\langle \beta_1 \rangle$. This implies that the generators must differ by a factor of associates, but previously we assumed that none of the beta-gamma pairs are associates. ↯

From part ii) we know that each principal ideal generated by an irreducible must factor into two prime ideals if it is not prime. The beta-ideal multiples decomposes into $2n$ prime ideals while the gamma-ideal multiples decompose into $2m$ prime ideals. Ideal factorization is unique, so it must be $2n = 2m$, but $n < m$. ↯

So the number of irreducibles in a factorization is invariant. □

neat!