Solution to Neukirch's Algebraic Number Theory

Yang

2023
Sep 20

Problem 1 $A \subseteq B$ be commutative rings, with B integral over A. Show that $B^* \cap A = A^*$
Solution: $(A^* \subset B^* \cap A)$ This is obvious.
$(B^* \cap A \subset A^*)$ For any $a \in B^* \cap A$, then there exists $b \in B$ such that $ab = 1$. As $b \in B$ is integral over A, there exists a monic polynomial with coefficients α_i in A for b: $b^n + \alpha_1 b^{n-1} + \cdots + \alpha_n = 0$. Multiplying a^n gives us the following one : $1^n + \alpha_1 a^1 + \cdots + \alpha_n a^n = 0$, after some transformation, we have $1 = -a(\alpha_1 + \cdots + \alpha_n a^{n-1})$ where $(\alpha_1 + \cdots + \alpha_n a^{n-1}) \in A$, so $a \in A^*$. Thus $B^* \cap A \subset A^*$.

Problem 2 Exercise 7 on page 15: The discriminant d_K of an algebraic number field K is always $\equiv 0 \pmod 4$ or $\equiv 1 \pmod 4$ (Stickelberger's discriminant relation).

The discriminate $d_K = d_{\mathcal{O}_K} = det((\sigma_i \omega_j))^2$ (assuming ω_j is the integral basis).
By the definition of discrimination, $det((\sigma_i \omega_j)) = \sum_{\pi \in S_n} sgn(\pi) \prod_{i=1}^n \sigma_i \omega_{\pi(i)} = \sum_{\pi \in A_n} \prod_{i=1}^n \sigma_i \omega_{\pi(i)} - \sum_{\pi \notin A_n} \prod_{i=1}^n \sigma_i \omega_{\pi(i)}$. By primitive element theorem, number field $K = Q(\theta)$ with all its conjugations in the form of $\sigma_i \theta$. In this way, $\omega_i = f_i(\theta)$ with $f_i \in Q\,[x]$, and $P = \sum_{\pi \in A_n} \prod_i \sigma_i \omega_{\pi(i)} = \sum_{\pi \in A_n} \prod_i f_{\pi(i)}(\sigma_i \theta)$, in the same way, $N = \sum_{\pi \notin A_n} \prod_i \sigma_i \omega_{\pi(i)} = \sum_{\pi \notin A_n} \prod_i f_{\pi(i)}(\sigma_i \theta)$.

As shown in the hint, what we need to do is to prove that $P + N$ and PN are integers. After action of elements in A_n on index of both P and N, nothing changes. While for elements not in A_n, P becomes Q and Q becomes P. So $P + N$ and PN, if we view them as polynomials for $x_i = \sigma_i \theta$, they are symmetrical polynomials, and because $f_i \in Q\,[x]$, so we have $PN,\ P + N \in Q\,[x]$ (viewed as polynomials for $x_i = \sigma_i \theta$ and considering that except $\sigma_i \theta$, everthing appearing in P and N are rational numbers, this can be done).

By symmetrical function theorem, (remember $\sigma_i \theta$ are roots for the minimal polynomial $g \in Q\,[x]$ for θ, and elementary symmetrical functions with indeterminates valued as $\{\sigma_i \theta\}$ is coefficient of this polynomial), $P + N, PN \in Q$, considering that they are integral over Q, they must be in $Q \cap \mathcal{O}_K = Z$. So
$(P - N)^2 = (P + N)^2 - 4PN \equiv 0, 1 (mod 4)$.

Problem 3 (a).If $g(\alpha)$ is dovisible by 3 in $Z\,[\alpha]$.
Then $g(\alpha) = 3h(\alpha)$ where $h = h_0 + h_1 x + \cdots + h_n x^n \in Z\,[x]$. So $g(\alpha) = 3h_0 + 3\alpha(h_1 + \cdots)$. And $g(\alpha) - 3h(\alpha) = 0$, thus $g(x) - 3h(x)$ has root α, and $g(x) - 3h(x) = \psi(x) f(x)$ (f is irreducible polynomial for α). Modulo 3, then we have $\bar{g}(x) - 0 = \bar{\psi}(x) \bar{f}(x)$. So $\bar{g}$ is divisible by $\bar{f}$ in $\mathbb{F}_3\,[x]$.

If $\bar{g}$ is divisible by $\bar{f}$ in $\mathbb{F}_3\left[x\right]$, then $\bar{f}(x)\bar{\phi(x)} = \bar{g}(x)$. Thus $(f(x)+3f'(x))(\phi(x)+3\phi'(x)) = g(x)+3g'(x)$ where $f', \phi', g' \in Z\left[x\right]$. Value x as α, then $f(\alpha)=0$, and $(3f'(\alpha))(\phi(\alpha)+3\phi'(\alpha)) - 3g'(\alpha) = g(\alpha)$. So obviously $g(\alpha)$ is divisible by 3.

(b). Now suppose that $\mathcal{O}_K = Z\left[\alpha\right]$, consider the four algebraic integers $\alpha_1 = (1+\sqrt{7})(1+\sqrt{10})$, $\alpha_2 = (1+\sqrt{7})(1-\sqrt{10})$, $\alpha_3 = (1-\sqrt{7})(1+\sqrt{10})$, $\alpha_4 = (1-\sqrt{7})(1-\sqrt{10})$. All products $\alpha_i\alpha_j$ will have factors $(1+\sqrt{7})(1-\sqrt{7}) = 1-7 = -6$ or $(1+\sqrt{10})(1-\sqrt{10}) = -9$ which are divisible by 3. For α_i, all its conjugates under Galois transformation are exactly $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ ($\sqrt{7} \leftrightarrow -\sqrt{7}$ and $\sqrt{10} \leftrightarrow -\sqrt{10}$).
Thus by definition, $Tr(\alpha_i^n) = \sum \alpha_i^n$. This is congruent to $(\alpha_1+\alpha_2+\alpha_3+\alpha_4)^n \pmod 3$ because in the expansion series of $(\alpha_1+\alpha_2+\alpha_3+\alpha_4)^n$, except α_i^n, all other terms contain $\alpha_i\alpha_j$ $(i \neq j)$ which is divisible by 3. And by calculation, $(\alpha_1+\alpha_2+\alpha_3+\alpha_4) = 4$, and $(1+3)^n \equiv 1\ (mod\ 3)$. So α^n is not divisible by 3, otherwise $Tr(3 \cdot \alpha_n/3)$ must be divisible by 3.

(c). For $\alpha_i\alpha_j = f_i(\alpha)f_j(\alpha_j)$ is divisible by 3, so by (a), $\bar{f}|\bar{f}_i\bar{f}_j$ (for $i \neq$j), in the same way, $\bar{f} \nmid \bar{f_i}^n$. Because $\mathbb{F}_3\left[x\right]$ is PID, then it is UFD, so $\bar{f}$ has an irreducible factor which does not divide $\bar{f}_i$ but does not divide all $\bar{f}_j$ (for $j \neq i$).

(d). By the above (c), we can see that $\bar{f}$ has at least four distinct irreducible factors over $\mathbb{F}_3$, but its degree must be over 4
(d). By the above conclusions, we can see that $\bar{f}$ has at least four distinct irreducible factors over $\mathbb{F}_3$ and the degree of field extension $Q(\sqrt{7}, \sqrt{10})$ is four, so the degree of f is at most 4. In this way, the degree of f can only be 4. However, this requires the (at least) four distinct irreducible factors of to be all of degree 1, however, over $\mathbb{F}_3$, there are only three irreducible polynomials of degree 1: $x-\bar{1}, x-\bar{2}, x-\bar{3}$. Thus, there must be one factor with degree at least 2, this leads to contradiction because $\bar{f}$ is thus of degree 5 but f is at most degree 4.

Problem 4
Solution:
For A is the finite module over Z, (and it is contained in a number field thus torsion free, so it must be free module over Z as Z os PID), take the generator set as $\{\lambda_i\}$, and $Z\left[\lambda_i\right]$ is submodule of A so it must be finitely generated as Z is PID. So λ_i is integral over Z.

Now take the fractional field of A as K, then K is subfield of K_0 and also a number field. Take the integral closure of Z in K, then it must be contained in A as integral closure of $A \supset Z$ in K is A, while it also contains A as the generators of A are all integral over Z so they are contained in the integral closure of Z. The proof is thus done, A is the integral closure of K.

Problem 3
Decompose $33+11\sqrt{-7}$ into irreducible integral elements of $Q(\sqrt{-7})$.

$33+11\sqrt{-7} = 11(3+\sqrt{-7})$ and $11 = (2+\sqrt{-7})(2-\sqrt{-7})$ where $2+\sqrt{-7}$ must be irreducible as its norm is exactly 11, nondecomposable.
For $3+\sqrt{-7}$, its decomposition may not be that obvious. The norm of $3+\sqrt{-7} = 16 = 2^4$, so it's

necessary to find some irreducible element with norm 2.
Take $\alpha = \frac{1+\sqrt{-7}}{2}$ into consideration, then $\alpha^2 - \alpha + 2 = 0$ and norm of α is 2, so it must be irreducible. Thus α is integral and $2 = -\alpha^2 + \alpha = \alpha(1-\alpha)$, so $3 + \sqrt{-7} = 2(\frac{3+\sqrt{-7}}{2})$. The norm of $\frac{3+\sqrt{-7}}{2}$ is $4 = 2^2$, indeed, $\frac{3+\sqrt{-7}}{2} = -(\frac{1-\sqrt{-7}}{2})^2$.
$33 + 11\sqrt{-7} = -(2+\sqrt{-7})(2-\sqrt{-7})(\frac{1+\sqrt{-7}}{2})(\frac{1-\sqrt{-7}}{2})^3$

Problem 5
Solution:
By the hint given, we shall consider the quotient $\mathcal{O}_K/p\mathcal{O}_K$.
By the course notes, if d is square free, the $\mathcal{O}_{\mathcal{Q}(\sqrt{d})} = Z\left[d\right]$ ($d \equiv 2, 3(\ mod\ 4)$) or $Z\left[\frac{1+\sqrt{d}}{2}\right]$ ($d \equiv 1\ (mod\ 4)$)
Take $Z\left[d\right]$ as the ring of integers. Then $\mathcal{O}_K = Z\left[x\right]/(x^2-d)$, so $\mathcal{O}_K/p\mathcal{O}_K = \mathbb{F}_p\left[x\right]/(x^2-\bar{d})$.
If $p\mathcal{O}_K = \prod_i \mathfrak{B}_i^{e_i}$ where $\mathfrak{B})i$ is prime ideal in $\mathcal{O}_K$.
lemma: $\left[Q(\sqrt{d}) : Q\right] = \sum_i e_i d_i$ where e_i is defined as above and $d_i = [\mathcal{O}_K/\mathfrak{B}_i : \mathbb{F}_p]$.
So there is at most two primes in the decomposition and the ramification index is at most two. $p\mathcal{O}_K = \mathfrak{B}_1^{e_1}\mathfrak{B}_2^{e_2}$ where $(e_1, e_2) = (1,1), (2,0) \cong (0,2), (1,0) \cong (0,1)$.
So by the chinese remainder theorem: $\mathcal{O}_K/p\mathcal{O}_K = \mathcal{O}/\mathfrak{B}_1^{e_1} \oplus \mathcal{O}/\mathfrak{B}_2^{e_2}$.
If $\bar{d} = 0$, then $\mathbb{F}_p\left[x\right]/(x^2)$ which contains nilpotent elemets which can only happen when ramification index is larger than 1.
If $x^2 \equiv d$ has nonzero solution, then $\mathbb{F}_p\left[x\right]/(x^2-\bar{d}) = \mathbb{F}_p\left[x\right]/(x-\bar{x_1}) \oplus \mathbb{F}_p\left[x\right]/(x-\bar{x_2})$ which is the case when $(e_1, e_2) = (1,1)$, which $p\mathcal{O}_K$ splits.
If $x^2 \equiv d$ has no solution mod d, then over $\mathbb{F}_p$, $x^2 - \bar{d}$ is irreducible and the quotient $\mathcal{O}_K/p\mathcal{O}_K$ is field, thus $p\mathcal{O}_K$ is prime.
For the remaining case, I am stuck and also curious about how to use the condition p does not divide $2d$.

Problem 6
The quotient $\mathcal{O}/\mathfrak{a}$ of a Dedekind ring $\mathcal{O}$ by an ideal $\mathfrak{a}$ is a principal ring.

Solution: $\mathfrak{a}$ can be factorized as product of prime ideals $\prod \mathfrak{p}_i^{n_i}$. By the Chinese Remainder Theorem, we can see that $\mathcal{O}/\mathfrak{a} = \oplus_i \mathcal{O}/\mathfrak{p}_i^{n_i}$. So it suffice to prove that $\mathcal{O}/\mathfrak{p}_i^{n_i}$ is a principal ring because product of principal ring is principal ring.
To prove that $\mathcal{O}/\mathfrak{p}^n$ is principal, we first notice that any proper ideal $\mathcal{I}$ containing $\mathfrak{p}^n$ satisfying $\mathcal{I}|\mathfrak{p}^n$, by the uniqueness of decomposition of ideals in Dedekind ring, $\mathcal{I}\mathfrak{p}\cdots\mathfrak{p} = \mathfrak{p}^n$, so $\mathcal{I}$ is in the form of $\mathfrak{p}^i$. Thus the proper ideals in $\mathcal{O}/\mathfrak{p}^n$ is in the form of $\mathfrak{p}/\mathfrak{p}^n \cdots \mathfrak{p}^{n-1}/\mathfrak{p}^n$. Besides, I want to mention that $\mathfrak{p}^i \neq \mathfrak{p}^j$ because of unique decomposition of ideals in the Dedekind ring
Denote the projection map $\pi : \mathcal{O} \to \mathcal{O}/\mathfrak{p}^n$, if $\pi(\mathfrak{p}) = \pi(\mathfrak{p}^2)$, then $\mathfrak{p}^2 + \mathfrak{p}^n = \mathfrak{p} + \mathfrak{p}^n$, so $\mathfrak{p} = \mathfrak{p}^2$. Thus $\mathcal{O}/\mathfrak{p}^n$ is a field which is definiely principal ideal ring.
If $\mathfrak{p} \neq \mathfrak{p}^2$, then for any $a \in \mathfrak{p}/\mathfrak{p}^2$, $(\pi(a)) \neq \mathfrak{p}^i/\mathfrak{p}^n$ for $i \geq 2$(otherwise $(a) + \mathfrak{p}^n = \mathfrak{p}^i \to\ a \in \mathfrak{p}^2$) So $(\pi(a)) = \mathfrak{p}/\mathfrak{p}^n$ and $(\pi(a)^i) = \mathfrak{p}^i/\mathfrak{p}^n$. Thus it's a principal ring. The proof is done.

Problem 7
$\mathfrak{m}$ is an integral ideal in the Dedekind ring $\mathcal{O}$, show that in each ideal class of Cl_K, there is an

integral ideal $\mathfrak{p}$ prime to $\mathfrak{m}$.

Solution: It suffices to find an element $u \in K^*$ such that $u\mathfrak{p}$ prime to $\mathfrak{m}$ for a fixed fractional ideal $\mathfrak{p}$.
As $\mathcal{O}$ is noetherian ring so there exists $c \in K^*$ such that $c\mathcal{O}$ is integral ideal. Denote the decomposition of $\mathfrak{m}$ as $\mathfrak{p}_1^{i_1} \cdots \mathfrak{p}_n^{i_n}$ with $(i_l > 0)$, and the integral ideal $c\mathfrak{p}$ can be decomposed as $\mathfrak{p}_1^{j_1} \cdots \mathfrak{p}_n^{j_n} \mathfrak{q}_1^{k_1} \cdots \mathfrak{p}_m^{k_m}$ with all upper indexes nonnegative. To construct an integral ideal equivalent but prime to $\mathfrak{m}$, we need to get rid of the factors $\mathfrak{p}_i$ in $c\mathfrak{p}$.
By the poof in problem 1, we can see that in quotient $\mathcal{O}/\mathfrak{p}^n$, all proper ideals in this quotient ring is generated by an arbitrary fixed element t in $\mathfrak{p} \setminus \mathfrak{p}^2$, and if $x \equiv t^i \bmod \mathfrak{p}^n$, then $(x)/\mathfrak{p}^n$=$(\bar{t})^i = \mathfrak{p}^i/\mathfrak{p}^n$. So for any $0 \leq m < n$, $\nu_{\mathfrak{p}}(t^m) = \nu_{\mathfrak{p}}(x) = m$, otherwise, $(x)/\mathfrak{p}^n = \mathfrak{p}^m/\mathfrak{p}$ will be some $\mathfrak{p}^i/\mathfrak{p}^n$ with $i > m$.
By the chinese remainder theorem, we can thus find an element $x \in \mathcal{O}$ such that for any $(i_1, \cdots, i_n)$ where i_k is nonnegative, and prime ideals $\mathfrak{p}_1 \cdots \mathfrak{p}_n$, the index $(\nu_{\mathfrak{p}_1} \cdots \nu_{\mathfrak{p}_n})$ of (x) is exactly $(i_1, \cdots, i_n)$.

Back to the integral ideal $c\mathfrak{p}$, we can find such an $x \in \mathcal{O}$ such that $\nu(x)$=$(j_1, \cdots, j_n, k_1 \cdots, k_m)$ with prime ideal factors as $(\mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{q}_1 \cdots \mathfrak{q}_m)$. Thus the decomposition of $x^{-1}c\mathfrak{p}$ has no factors as $\mathfrak{p}_i$.
While we successfully eliminate the factors such as $\mathfrak{p}^i$, there may be factors with negative indexes, thus we denote $x^{-1}c\mathfrak{p} = \mathfrak{r}_1^{-d_1} \cdots \mathfrak{r}_l^{-d_l}$ with $d_i \geq 0$.
Again we can find $y \in \mathcal{O}$ such that for prime ideal factors $(\mathfrak{p}_1, \cdots, \mathfrak{p}_n, \mathfrak{r}_1 \cdots, \mathfrak{r}_l)$ and index of (y) for these factors is $(0, \cdots, 0, d_1 \cdots, d_l)$. Thus multiplying y eliminates negative factors in $x^{-1}c\mathfrak{p}$, so $yx^{-1}c\mathfrak{p}$ has no factors $\mathfrak{p}_i$ and is indeed an integral ideal.

Problem 8
Let I and a be ideals of A, with prime factorizations

$$I = \prod_{\mathfrak{p}} p^{\nu(p)} \quad \text{and } \mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha(\mathfrak{p})}.$$

(1)Show that $I \supseteq \mathfrak{a}$ if and only if $\nu(\mathfrak{p}) \leq \alpha(\mathfrak{p})$ for all $\mathfrak{p}$.
(2) Let $\mathfrak{a}$ and $\mathfrak{b}$ be nonzero ideals of A. Carefully prove that the ideal $\mathfrak{a} + \mathfrak{b}$ equals $\gcd(\mathfrak{a}, \mathfrak{b})$. Here, the gcd is defined in the obvious way using the prime factorizations of $\mathfrak{a}$ and $\mathfrak{b}$. Indeed, write

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha(\mathfrak{p})} \quad \text{and } \mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{\beta(\mathfrak{p})},$$

where the product is over all (distinct) nonzero prime ideals of A. Then $\gcd(\mathfrak{a}, \mathfrak{b}) = \prod_{\mathfrak{p}} \mathfrak{p}^{\min\{\alpha(\mathfrak{p}), \beta(\mathfrak{p})\}}$.

Solution:
(1). $(\Leftarrow)$ If $\nu(\mathfrak{p}) \leq \alpha(\mathfrak{p})$, then $\mathfrak{p}^{\alpha(\mathfrak{p})} \subset \mathfrak{p}^{\nu(\mathfrak{p})}$, thus we have $I \supset \mathfrak{a}$
$(\Rightarrow)$ If $I \supset \mathfrak{a}$, then by definition, $I^{-1}\mathfrak{a} \subset \mathcal{O}$.That is $\prod_{\mathfrak{p}} \mathfrak{p}^{-\nu(\mathfrak{p})+\alpha(\mathfrak{p})}$ is an integral ideal, thus all its index must be nonnegative by the decomposition theorem. so $\nu(\mathfrak{p}) \leq \alpha(\mathfrak{p})$

(2).First of all, it's obvious that $\mathfrak{p}^{min\{\alpha(\mathfrak{p}), \beta(\mathfrak{p})\}} \supset \mathfrak{p}^{\alpha(\mathfrak{p})}$ and $\mathfrak{p}^{min\{\alpha(\mathfrak{p}), \beta(\mathfrak{p})\}} \supset \mathfrak{p}^{\beta(\mathfrak{p})}$. Thus $gcd(\mathfrak{a}, \mathfrak{b})$ contains both $\mathfrak{a}$ and $\mathfrak{b}$. Thus $gcd(\mathfrak{a}, \mathfrak{b}) \supset \mathfrak{a} + \mathfrak{b}$

It suffices now to prove that $\mathfrak{a}+\mathfrak{b} \supset gcd(\mathfrak{a},\mathfrak{b})$. Keep in mind that the definition of $\mathfrak{a}+\mathfrak{b}$ means that it is the smallest ideals containing both $\mathfrak{a}$ and $\mathfrak{b}$. Thus if the $\mathfrak{a}+\mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mu(\mathfrak{p})}$ with $\mu(\mathfrak{p}) < min(\nu(\mathfrak{p}), \alpha(\mathfrak{p}))$, there is a contradiction that $\mathfrak{a}+\mathfrak{b} \underset{\neq}{\supseteq} gcd(\mathfrak{a},\mathfrak{b}) \underset{\neq}{\supseteq} \mathfrak{a}+\mathfrak{b}$. Thus $\mathfrak{a}+\mathfrak{b} \supset gcd(\mathfrak{a},\mathfrak{b})$. Thus $gcd(\mathfrak{a},\mathfrak{b}) = \mathfrak{a}+\mathfrak{b}$.

Problem 9
Show that Minkowski's lattice point theorem can not be improved. And if X is compact, the statement remains true.(Let Γ be a complete lattice in the euclidean space V and X a centrally symmetric, convex **compact** subset of V. Suppose that Vol(X)$\geq 2^n$Vol(γ), then X contains at least one nonzero lattice point))
Solution: here is an example, the lattices $\Gamma = \lambda Z$ and Vol(Γ) $= \lambda$. Then the interval $(-\lambda, \lambda)$ has volume 2Vol(Γ) $= 2\lambda$, $(-\lambda, \lambda)$ has no nonzero lattice point.
If X is compact, consider the dilate $X_\epsilon = (1+\epsilon)X$ with $\epsilon > 0$, then $X = \cap_\epsilon X_\epsilon$. Indeed, if $X \underset{\neq}{\supseteq} \cap_\epsilon X_\epsilon$, then for any such element $z \in \cap_\epsilon X_\epsilon \setminus X$, we have $\frac{z}{1+\epsilon} \in X$, and by the compactness, the family $\frac{z}{1+\epsilon}$ has its limit point in X, that is $z \in X$. Contradiction! And obviously $X \subset \cap_\epsilon X_\epsilon$, so we have $X = \cap_\epsilon X_\epsilon$.
And for $\epsilon = 1$, that is X_1, which is bounded, so there are at most finite lattice points in X_ϵ with $\epsilon \in (0,1)$(because X is centrally symmetric and convex, so it must contains 0, and thus such dilation must form a nest, that is , $X_\epsilon \subset X_{\epsilon'}$ for $\epsilon < \epsilon'$). And for each X_ϵ, we can use the Minkowski theorem because the inequality is strict, so X_ϵ contains a lattice point nonzero, and because each of these lattice points must be contained in X_1 so there are only finite choices, thus we can pick an infinite series of $\epsilon_i \in (0,1)$ such that there is a fixed lattice point $p \in X_{\epsilon_i}$ for $i = 1 \cdots n \cdots$. And by the property $X_\epsilon \subset X_{\epsilon'}$ for $\epsilon < \epsilon'$, we can see that $p \in X_\epsilon$ for all $\epsilon > 0$. Thus $p \in \cap_\epsilon X_\epsilon$=$X$.
Thus the Minkowski theorem still makes sense.

Problem 10 (Minkowski's Theorem on Linear Forms)
Fact: linear transformation remains the property of convexity (centrally), boundedness, and symmetry.
Consider the box B:$\{(x_1, \cdots, x_n) || x_i| < c_i\}$, which is a symmetric convex(centrally) and bounded set, thus after the linear transformation, $A^{-1}B$ is again centrally symmetric, symmetric and bounded. By the basic measure theory, $m(A^{-1}B) = det(A^{-1})m(B)$=$2^n det(A^{-1}) \prod_i c_i$> 2^n. Thus by the Minkowski theorem, there exists an integer point p in the form $(g_1, \cdots, g_n)$ with $g_i \in Z$ in this set $A^{-1}B$. Thus $A \cdot p \in B$.

Problem 11 Write down a constant A which depends only on K such that every integral ideal $\mathfrak{a} \neq 0$ of K contains an element $a \neq 0$ satisfying $|\tau a| < A(\mathfrak{o}_K : \mathfrak{a})^{1/n}$ for all $\tau \in Hom(K, C)$.
Solution: let $c_\tau = A(\mathfrak{o}_K : \mathfrak{a})^{1/n}$. Then if $\prod_\tau c_\tau > (\frac{2}{\pi})^s \sqrt{|d_K|}(\mathfrak{o}_K : \mathfrak{a})$, by the theorem (5.3) in Neukirch, there exists $a \in \mathfrak{a}$ that $a \neq 0$ and $|\tau a| < c_\tau$. So we just need to make sure that $A^n > (\frac{2}{\pi})^s \sqrt{|d_K|}$. For instance, $A = (\frac{5}{\pi})^{s/n} \sqrt[2n]{|d_k|}$.

Problem 12 Show that $\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\}$ is an integral basis of $\mathbb{Q}(\sqrt[3]{2})$.

Solution: First of all, it's obvious that $Z[\sqrt[3]{2}] \subset \mathcal{O}_K$. And more precisely, by the field extension theory, $\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\}$ is a basis for $L|K$, thus $d(Z[\sqrt[3]{2}]) = d(1, \sqrt[3]{2}, \sqrt[3]{2^2}) = (\sqrt[3]{2}-1)^2(\sqrt[3]{2^2}-1)^2(\sqrt[3]{2^2}-\sqrt[3]{2})^2 = -108 = -2^2 3^3$. Thus $d(Z[\sqrt[3]{2}]) = (\mathfrak{o}_K : Z[\sqrt[3]{2}])^2 d(\mathfrak{o}_K)$, so any integral element α satisfies

$6\alpha = x_1 + x_2\sqrt[3]{2} + x_3\sqrt[3]{2^2}$ with $x_i \in Z$.
Now it's time to reduce the number of different cases.
For any integer $z \in Z$ with property $\sqrt[3]{2}|z$ in $\mathfrak{o}$, then there exists integral element ω over $\mathbb{Q}$ such that $\omega\sqrt[3]{2} = z$, then $\omega^3 2 = z^3$ and $\omega^3 = z^3/2 \in \mathbb{Q}$. So $\omega \in \mathbb{Q} \cap \mathfrak{o}_K = Z$. Thus $2|z^3$ in integer ring Z and so $2|z$ as integers. So for $x_1 : x_1 = 6\alpha - x_2\sqrt[3]{2} - x_3\sqrt[3]{2^2}$. In $\mathfrak{o}_K : \sqrt[3]{2}|x_1$, so $2|x_1$, and again by induction, $\sqrt[3]{2}^2|\sqrt[3]{2}x_2$, so $\sqrt[3]{2}|x_2$, and $2|x_2$, in the same way, $2|x_3$.
So now we only need to consider the case: $\alpha = \frac{y_1+y_2\sqrt[3]{2}+y_3\sqrt[3]{2^2}}{3}$ with $y_i \in Z$.

To prove that $\alpha \in Z[\alpha]$, we only need to examine (y_1, y_2, y_3) with $y_i = 0, 1, 2$ which is the mod 3 classes. First we consider the most special case: $(1, 1, 1)$. Then the norm of $N(1 + \sqrt[3]{2} + \sqrt[3]{2}) = 1$, thus $N(\frac{1+\sqrt[3]{2}+\sqrt[3]{2^2}}{3}) = 1/27$ which is not integral, and so is $(2, 2, 2)$. Now we have excluded the cases when all y_i is equal.

For the remaining case: I believe calculating the norm will lead to contradiction to integrality. But I really can't come up with any methods of doing this.
I do feel like using the condition that $x = y_1 + y_2\sqrt[3]{2} + y_3\sqrt[3]{2^2}$ is integral is more than using the condition that the norm is integral. Consider the polynomial for x, which degree must be 1 or 3, ($(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(x))(\mathbb{Q}(x) : Q) = 3$), then the case of degree 1 is easily done, for the case of cubic extension: the cubic polynomial minimal for x $x^3 + a_1x^2 + x_2x + a_3 = 0$ with $a_i \in Z$. And I guess the integrality of a_i will limit the choice of y_i, but I am not very familiar with cubic equation and its galois group, especially for the case when the coefficient of x^2 is not vanishing.

Problem 4 Let $\mathfrak{a}$ be an integral ideal of K and $\mathfrak{a}^m = (a)$. Show that $\mathfrak{a}$ become a principal ideal in the field extension $L : K(\sqrt[m]{a})$.

For $\mathfrak{a}\mathfrak{o}_L$, take m power: $\mathfrak{a}^m\mathfrak{o}_L = (a)\mathfrak{o}_L$. Thus by the prime decomposition of ideals :$\mathfrak{a}^m\mathfrak{o}_L = (\sqrt[m]{a})^m$, and take a decomposition for $\mathfrak{a}\mathfrak{o}_L = \mathfrak{q}_i \cdots \mathfrak{q}_k$ and $(\sqrt[m]{a}) = \mathfrak{p}_1 \cdots \mathfrak{p}_l$. So $\mathfrak{q}_1^m \cdots \mathfrak{q}_k^m = \mathfrak{p}_1^m \cdots \mathfrak{p}_l^m$. Thus by the uniqueness of prime decomposition, we have $\mathfrak{a}\mathfrak{o}_L = (\sqrt[m]{a})$ which is principal.

Problem 5 Show that, for every number field K, there exists a finite extension L such that every ideal of K becomes a principal ideal.

Solution: By theorem (6.3), there are only finite ideal classes in $\mathfrak{o}_K$, we denote them as $\bar{\mathcal{I}}_1, \cdots, \bar{\mathcal{I}}_n$, here the representative $\mathcal{I}_i$ is chosen in the class to be integral ideal. By the finiteness of class number, there exists some $n < m$ such that $\mathcal{I}_i^n \sim \mathcal{I}_i^m$ such that they both lie in the same ideal class, since $\mathcal{I}_i^m \subset \mathcal{I}_i^m$, so $\mathcal{I}_i^m\mathcal{J} = \mathcal{I}_i^n$ where $\mathcal{J}$ is an integral ideal, and also since they are in the same ideal class, so $\mathcal{J}$ is a principal ideal (a_i), generated by an element $a_i \in \mathfrak{o}_K$. Thus $\mathcal{I}_i^{m-n} = (a_i)$, by the problem 4, there exists finite field extension $L_i = K(\alpha_i)$ over K such that $\mathcal{I}_i$ becomes principal in L_i. And also, all the other integral ideals $\mathcal{P} \sim \mathcal{I}_i$ in the same class as $\mathcal{I}_i$, after the field extension, firstly, they are still the integral ideals in the same class as $\mathcal{I}_i\mathfrak{o}_L$, secondly, as $\mathcal{P} = \mathcal{I}_i(b)$ where $b \in \mathfrak{o}_K$ is integral, so after field extension: $\mathcal{P}\mathfrak{o}_{L_i} = (b)\mathcal{I}_i\mathfrak{o}_L$, thus all the other integral ideals after extension become integral principal ideals.

Since principal ideal after field extension is still principal, we can do this by induction: for $\mathcal{I}_1$, there exists finite field extension: $L_1 = K(\alpha_1)$ such that $\mathcal{I}_1$ and all the other integral ideals in the same class as it is principal in this extension, and again by induction for the remaining $i = 2, \cdots, n$. In then end, we will have finite field $L|K$ such that all the original ideals in $\mathfrak{o}_K$ is principal

Problem 1 Let K be a totally real number field, i.e., $X = Hom(K, \mathbb{C}) = Hom(K, \mathbb{R})$, and let T be a proper nonempty subset of X. Then there exists a unit ϵ satisfying $0 < \tau\epsilon < 1$ for $\tau \in T$, and $\tau\epsilon > 1$ for $\tau \notin T$.
Solution:
Recall the following lemma used in class to prove the Dirichchlet theorem.

Lemma 1 For every $\tau_0 : K \to \mathbb{C}$, there is a unit $u \in \mathcal{O}_K^*$ such that $|\tau(u)| < 1$ for any $\tau \neq \tau_0, \bar{\tau}_0$ and $|\tau_0(u)| = |\bar{\tau}_0(u)| > 1$

Lemma 2 Inspired by this lemma, in our totally real number field case, we could try to imitate this lemma: for all the embeddings of K into C, (actually there only exists real embeddings) we denoted as $\rho_1, \rho_2 \cdots \rho_n$, and for any proper subset $T \subset Hom(K, \mathbb{C})$, there exists a unit $\epsilon \in \mathcal{O}_K^*$ such that $|\tau(\epsilon)| < 1$ for $\tau \in T$ and $|\tau(\epsilon)| > 1$ for $\tau \notin T$.
Proof:
Step 1: First of all, we can construct a series of $\{\alpha_m\}$

Problem 3 Let $f : A \to B$ be a ring homomorphism of rings and S a multiplicatively closed subset such that $f(S) \subset B^*$. Then f induces a homomorphism of rings: $A_S \to B$.

Solution: Here I try to prove a stronger version which can be used in the problem 2. If the condition of f is satisfied as $f(S) \subset B^*$, then there exists a unique $g : A_S \to B$ as shown in the diagram

$$\begin{tikzcd} & B \\ A \arrow[ur, "f"] \arrow[r, "i"] & A_S \arrow[u, dashed, "g"] \end{tikzcd}$$

Uniqueness is easily proven, since $g(a/s) = g(a/1)g(1/s)$.
Now let's prove the existence: Define $g(a/s) = f(a)f(s)^{-1}$, then g will clearly be a ring morphism. Suppose that $a/s = a'/s'$, then there exists $t \in S$ such that $t(as' - a's) = 0$, thus $f(t)(f(a)f(s') - f(a')f(s)) = 0$ since $f(t)$ is a unit, so $f(a)f(s') - f(a')f(s) = 0$ so we have $f(a)f(s)^{-1} = f(a')f(s')^{-1}$. Thus this is a well defined ring morphism and unique.

Problem 2
Let S and T be two multiplicative subsets of A, and T^* the image of T in A_S. Then one has $A_{ST} \cong (A_S)_{T^*}$.
Solution: By the natural morphism: $i : A \to A_S \to (A_S)_{T^*}$, then $i(ST)$ are all units in the ring $(A_S)_{T^*}$, thus by the problem above, we have a natural morphism induced by this: $g : A_{ST} \to$

$(A_S)_{T^*}$. Now it's left to prove this morphism is isomorphism.
First of all, surjectivity is obvious, for any $\frac{i(a)/i(s)}{i(t)} \in (A_S)_{T^*}$, then a/st is sent to this element by g.
Now it's left to prove the injection, if a/st is sent to $0 \in (A_S)_{T^*}$, then there exists $\bar{t'} \in T^*$ which is the image of $t' \in T$ under the morphism: $A \to A_S$ such that $\bar{t'}a = 0 \in A_S$, thus there exists $s' \in S$ such that $s't's = 0 \in A$, so $a/st = 0 \in A_{ST}$. Thus the morphism is injective and it is isomorphism.

Problem 4
Let A be an integral domain. If the localization A_S is integral over A, then $A_S = A$.
If A is integral, any localization ring A_S over A is still integral in the sense that if $\frac{a}{s}\frac{a'}{s'} = 0$ then there exists $s'' \in S$ such that $s''aa' = 0$, because $s'' \neq 0$ so a or a' is zero. So the natural morphism $A_S \to (A_S)_{T^*}$ is injective.
And consider the multiplicative set $T = A \setminus (0)$ and the corresponding localization ring $A_T = Frac(A)$, then for any other multiplicative set S, we have $S \subset T$ so $ST = T$, by the above problem, we have a natural isomorphism $A_T \cong (A_S)_{T^*}$. So for any localization ring A_S, there is a natural inclusion of this localization ring into the fractional field.
Now we can talk all the rings A and A_S, viewed them as subrings of the fractional field $Frac(A)$. Thus if A_S is integral over A, then for any $s \in S$, we have an integral equation for $\frac{1}{s}$, $(\frac{1}{s})^n + a_1(\frac{1}{s})^{n-1} + \cdots + a_n = 0$, thus $1 = -s(a_1 \cdots a_n s^{n-1}) \in A$ so s is a unit in A and thus all elements $a/s \in A$, so $A_S = A$
Problem 1. Let $K = Q(\sqrt{223})$
(a).Find the fundamental unit.
(b). Compute the class group of K and describe the relation of the class group's generators.

Proof. (a). Because $223 \equiv 3 \bmod 4$, so the ring of integers is exactly the $Z[\sqrt{223}]$ by exercise 2.4, and for a unit $a + b\sqrt{223} \in Z[223]$, then absolute norm is ± 1. Unwinding the definition, we have $a^2 - 223b^2 = \pm 1$ where $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, and $(224 - 15\sqrt{223})$ is a solution for this Pell's equation, and it suffices to prove that this is the 'fundamental unit'.
By the Dirichlet's unit theorem, any unit is the product of group of roots of units in K and some free abelian group of rank 1. So if $224 - 15\sqrt{223}$ is not the generator, then there is another fundamental unit $c + d\sqrt{223} \in Z[\sqrt{223}]$ such that $224 - 15\sqrt{223} = \nu(c + d\sqrt{223})^n$ where ν is a root of unit in the field $K = Q(\sqrt{223})$, and the only possible choice is ± 1. Take a closer look at the $(c+d\sqrt{223})^n = c^n + \cdots + \binom{n}{k}c^{n-k}d^k(\sqrt{223})^k + \cdots + d^n(\sqrt{223})^n$, the coefficient of $\sqrt{223}$ must have a factor d, so $d = \pm 1, \pm 3, \pm 5, \pm 15$. After taking these values in, we can easily check that the only possible d is ± 15 and $c = \pm 224$. So $224 - 15\sqrt{223}$ is fundamental unit.
(b). The Minkowski bound $(\frac{2}{\pi})^1\sqrt{|4 \cdot 223|} \leq 20$. So we only need to consider the prime ideal $\mathcal{P}$ in $Z[\sqrt{223}]$ such that $\mathcal{P} \cap Z = (p)$ with prime number $p \leq 20$.
(1) $p = 2$, $(x^2 - 223) \equiv (x^2 - 1) \equiv (x - 1)^2 \pmod 2$, the prime ideals lying over (2) are$(\sqrt{223} - 1, 2)$

(2) $p = 3$, $(x^2 - 223) \equiv (x^2 - 1) \equiv (x - 1)(x + 1) \pmod 3$, the prime ideals lying over (3) are $(\sqrt{223} - 1, 3)$ and $(\sqrt{223} + 1, 3)$
(3) $p = 5$, $(x^2 - 223) \equiv (x^2 - 3) \pmod 5$, no roots, the prime ideal (5) is inert.
(4) $p = 7$, $(x^2 - 223) \equiv (x^2 - 6) \pmod 7$, no roots, the prime ideal (7) is inert.
(5) $p = 11$, $(x^2 - 223) \equiv (x^2 - 223) \equiv (x - 6)(x - 5)(\text{mod } 11)$, the prime ideals lying over are $(\sqrt{223} - 6, 11)$ and $(\sqrt{223} - 5, 11)$

(6) $p = 13$, $(x^2 - 223)$ has no roots, the prime ideal (13) is inert.
(7) $p = 17$, $(x^2 - 223) \equiv (x-6)(x-11)$ has no roots, the prime ideals lying over (17) is $(\sqrt{223}-6, 17)$ and $(\sqrt{223} - 8, 17)$.
(8) $p = 19$, $(x^2 - 223)$ has no roots (mod 19), the prime ideal (19) is inert.
The nontrivial prime ideal candidates are $(\sqrt{223}+1, 2), (\sqrt{223}+1, 3), (\sqrt{223}-6, 11), (\sqrt{223}-11, 17)$ and of course their conjugates ideals as inverse elements.
The absolute norm of $(\sqrt{223} + 1, 2)^2$ is 2^2 where 2 is inertia degree, so $(\sqrt{2} - 1, 2)$'s norm is only possible for 2. And $\sqrt{223} - 1 + 2 \times 8 = 15 + \sqrt{223}$ which norm is 2 and contained in $(\sqrt{223} - 1, 2)$ and thus $(\sqrt{223} - 1, 2) = (\sqrt{223} + 15)$.
The absolute norm of $(\sqrt{223} + 1, 3)$ is 3^1 where 1 is inertia degree, and $(\sqrt{223} - 6, 11)$ is 11, so the norm of $(\sqrt{223} + 1, 3)(\sqrt{223} - 6, 11)$ is $33{=}(33 + 223 - 223) = 256 - 223 = 16^2 - 223 = (16 - \sqrt{223})(16 + \sqrt{223})$. And $(\sqrt{223} + 1, 3)(\sqrt{223} - 6, 11) = (11\sqrt{223} + 11, 3\sqrt{223} - 18, 33, 217 - 5\sqrt{223}) = (16 + \sqrt{223}, 33)$, so $(16 + \sqrt{223})$ is in this ideal and has the same norm with it, so $(16 + \sqrt{223}) = (\sqrt{223} + 1, 3)(\sqrt{223} - 6, 11)$.
In the same way, the absolute norm of $(\sqrt{223} - 11, 17)(\sqrt{223} + 1, 3)$ is $51{=}2^2 223 - 29^2 = (2\sqrt{223} - 29)(2\sqrt{223}+29)$. $(\sqrt{223}-11, 17)(\sqrt{223}+1, 3) = (212-10\sqrt{223}, 51, 3\sqrt{223}-33, 17\sqrt{223}-33, 17\sqrt{223}+17) = (-\sqrt{223} - 91, 51, 2\sqrt{223} + 182) = (2\sqrt{223} + 29, \sqrt{223} - 91, 51)$, so $(2\sqrt{223} + 29)$ is in the ideal product and has the same norm as it, so $(\sqrt{223} - 11, 17)(\sqrt{223} + 1, 3)$ is also principal.
By the above calculation, we can see that the only main character is actually the prime ideals lying over (3): $(\sqrt{223} + 1, 3)$, and all the other candidates are either principal (prime ideals over (2)), or they are the inverse of it (their product is principal ideal).
So the class group is generated the ideal $(\sqrt{223} + 1, 3)$ and it suffices to find the order of it.
$(\sqrt{223} + 1, 3)^2 = (9, 3 + 3\sqrt{223}, 224 + 2\sqrt{223}) = (9, 3 + 3\sqrt{223}, 224 + 2\sqrt{223} - 9 \times 25) = (9, 3 + 3\sqrt{223}, -1 + 2\sqrt{223}) = (9, (3 + 3\sqrt{223}) + 3(-1 + 2\sqrt{223}), -1 + 2\sqrt{223}) = (-1 + 2\sqrt{223}, 9)$, and again $(-1 + 2\sqrt{[223}, 9)(\sqrt{223} + 1, 3) = (14 - \sqrt{223})$.
So we can see that the order of $(\sqrt{223} + 1, 3)$ is factor of 3, so it is either 1 or 3.
It now suffices to prove that $(\sqrt{223} + 1, 3)$ is not principal. This is actually the Pell equation: $x^2 - 223y^2 = \pm 3$, and by the reciprocity formula, $(\frac{3}{223}) = -1$, so there is no solution (here we use the conclusion in problem 3 below) for +3.
For -3, the above method doesn't work out because $(\frac{-1}{3}) = -1$, we assume that there is a corresponding generator (a) ,then $(\sqrt{223} - 1) = ab$, so b is a solution to the pell equation with norm 3*37, but $(\frac{3 \times 37}{223}) = -1$, so there is no solution.
So this class group is actually a cyclic group C_3

□

Problem 2. Let $(a, p) = 1$, and $a\nu \equiv r_\nu \bmod p$, $\nu = 1, \cdots, p-1$, $1 \leq r_\nu \leq p-1$, the permutation π corresponding to this has $sgn(\pi) = (\frac{a}{p})$.

Proof. As a permutation, π can be decomposed into cycles in the form $(x, ax, a^2x, \cdots, a^{k-1}x)$ where k is the order of a in the multiplicative group $\mathbb{F}_p^\times$. Because this permutation is induced by the multiplication of a, so all the cycles in π has the same length k, and there are $\frac{p-1}{k}$ components, and the sign is $((-1)^{k-1})^{\frac{p-1}{k}} = \text{sgn}(\pi_a) = \left((-1)^{k-1}\right)^{\frac{p-1}{k}} = \begin{cases} (-1)^{\frac{p-1}{k}} & \text{if } k \text{ is even} \\ \\ 1 & \text{if } k \text{ is odd} \end{cases}$

By the Euler's criterion (shown in the textbook), $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}$.
When k is even, recall that $a^k = 1 = (a^{\frac{k}{2}})^2$, $(a^{\frac{k}{2}} - 1)(a^{\frac{k}{2}} + 1) \equiv 0$, thus $a^{\frac{k}{2}} \equiv -1\ mod(p)$ because k is the order of a so $a^{\frac{k}{2}} \neq 1 \in \mathbb{F}_p$. Thus $a^{\frac{p-1}{2}} = (a^{\frac{k}{2}})^{\frac{p-1}{k}} = (-1)^{\frac{p-1}{k}} = sgn(\pi)$.
When k is odd, recall that $2|p-1$, so $\frac{p-1}{2k} \in \mathbb{Z}$, so $a^{\frac{p-1}{2}} = (a^k)^{\frac{p-1}{2k}} = 1{=}sgn(\pi)$

□

Problem 3. Legendre form $(\frac{3}{p})$ totally depends on the class of p mod 12.

Proof. By reciprocity formula, we can see that $(\frac{3}{p})(\frac{p}{3}) = (-1)^{\frac{p-1}{2}\frac{3-1}{2}} = (-1)^{\frac{p-1}{2}}$ which is 1 if $p \equiv 1\ mod(4)$ and is -1 if $p \equiv 3\ mod(4)$.
By Euler's criterion, $(\frac{p}{3}) = (p)^{\frac{3-1}{2}}\ mod(3){=}p\ mod(3)$.
So $(\frac{3}{p})$ is determined by $p\ mod(3)$ and $p\ mod(4)$. Thus it is determined by mod 12 class. □