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 $\mathbb{F}_3[x]$, 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 $f', \phi', g' \in Z[x]$. 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 $\mathcal{O}_K = Z[\alpha]$, 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 $\mathbb{F}_3[x]$ 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 $Z[\lambda_i]$ 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 $\mathcal{O}_{\mathcal{Q}(\sqrt{d})} = Z[d]$ $(d \equiv 2, 3(\ mod\ 4))$ or $Z\left[\frac{1+\sqrt{d}}{2}\right]$ $(d \equiv 1\ (mod\ 4))$
Take $Z[d]$ as the ring of integers. Then $\mathcal{O}_K = Z[x]/(x^2-d)$, so $\mathcal{O}_K/p\mathcal{O}_K = \mathbb{F}_p[x]/(x^2-\bar{d})$.
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 $\mathbb{F}_p[x]/(x^2)$ which contains nilpotent elemets which can only happen when ramification index is larger than 1.
If $x^2 \equiv d$ has nonzero solution, then $\mathbb{F}_p[x]/(x^2-\bar{d}) = \mathbb{F}_p[x]/(x-\bar{x_1}) \oplus \mathbb{F}_p[x]/(x-\bar{x_2})$ 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 $\mathfrak{a}+\mathfrak{b} \supsetneqq gcd(\mathfrak{a},\mathfrak{b}) \supsetneqq \mathfrak{a}+\mathfrak{b}$. 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 $\mathrm{Vol}(\Gamma) = \lambda$. Then the interval $(-\lambda, \lambda)$ has volume $2\mathrm{Vol}(\Gamma) = 2\lambda$, $(-\lambda, \lambda)$ 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 $X \supsetneqq \cap_\epsilon X_\epsilon$, 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.