Math 129 Problem Set 5

Lev Kruglyak

March 29, 2022

For any number field K, we'll use $\mathcal{O}_K$ to denote the ring of integers of K, i.e. $\mathcal{O}_K = \mathbb{A} \cap K$. Also let $\Delta(\cdots)$ be the discriminant. We'll use Δ_K to mean the discriminant of a number field K.

I collaborated with Ignasi Segura Vicente on this problem set.

Problem 2.8.

(a) Let p be an odd prime and $\zeta_p = e^{2\pi i/p}$. Show that

$$\sqrt{(-1)^{\frac{p-1}{2}} p} \in \mathbb{Q}[\zeta_p].$$

Express $\sqrt{-3}$ and $\sqrt{5}$ in the appropriate $\mathbb{Q}[\zeta_p]$.

(b) Show that the 8^{th} cyclotomic field contains $\sqrt{2}$.

(c) Show that every quadratic number field K is contained in $\mathbb{Q}[\zeta_d]$ where $d = |\Delta_K|$.

(a) Recall that for any odd prime p we have

$$\Delta_{\mathbb{Q}[\zeta_p]} = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

However by definition of discriminant, we know that $\Delta_{\mathbb{Q}[\zeta_p]} = \alpha^2$ where $\alpha \in \mathbb{Q}[\zeta_p]$ is the determinant of the discriminant matrix. So

$$(-1)^{\frac{p-1}{2}} p = \frac{\Delta_{\mathbb{Q}[\zeta_p]}}{p^{p-3}} = \frac{\alpha^2}{p^{p-3}} = \left(\frac{\alpha}{p^{(p-3)/2}}\right)^2.$$

Thus $\sqrt{(-1)^{\frac{p-1}{2}} p} \in \mathbb{Q}[\zeta_p]$ as desired. To find $\sqrt{-3}$, we let $p = 3$, $\zeta = \zeta_3$ and use the derived formula for $\sqrt{-3}$, i.e.

$$\sqrt{-3} = \frac{1}{3^{(3-3)/2}} \begin{vmatrix} \sigma_1(\zeta) & \sigma_1(\zeta^2) \\ \sigma_2(\zeta) & \sigma_2(\zeta^2) \end{vmatrix} = \begin{vmatrix} \zeta & \zeta^2 \\ \zeta^2 & \zeta \end{vmatrix} = \zeta^2 - \zeta^4 = \zeta^2 - \zeta$$

Where $\sigma_i \in \mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q})$ is the automorphism sending z to z^i. Checking the square $(\zeta^2 - \zeta)^2 = \zeta - 2 + \zeta^2 = -3$ confirms the formula. Next for $\sqrt{5}$, set $p = 5$ and $\zeta = \zeta_5$. Then

$$\sqrt{5} = \frac{1}{5^{(5-3)/2}} \begin{vmatrix} \sigma_1(\zeta) & \sigma_1(\zeta^2) & \sigma_1(\zeta^3) & \sigma_1(\zeta^4) \\ \sigma_2(\zeta) & \sigma_2(\zeta^2) & \sigma_2(\zeta^3) & \sigma_2(\zeta^4) \\ \sigma_3(\zeta) & \sigma_3(\zeta^2) & \sigma_3(\zeta^3) & \sigma_3(\zeta^4) \\ \sigma_4(\zeta) & \sigma_4(\zeta^2) & \sigma_4(\zeta^3) & \sigma_4(\zeta^4) \end{vmatrix} = \frac{1}{5} \begin{vmatrix} \zeta & \zeta^2 & \zeta^3 & \zeta^4 \\ \zeta^2 & \zeta^4 & \zeta & \zeta^3 \\ \zeta^3 & \zeta & \zeta^4 & \zeta^2 \\ \zeta^4 & \zeta^3 & \zeta^2 & \zeta \end{vmatrix} = 2\zeta^3 + 2\zeta^2 + 1.$$

As before, a simple check confirms that $(2\zeta^3 + 2\zeta^2 + 1)^2 = 5$.

(b) Let $\zeta = \zeta_8$ and consider $\zeta + \zeta^{-1}$. Then $(\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = 2$, so $\sqrt{2} \in \mathbb{Q}[\zeta_8]$.

(c) For brevity, we'll write $\zeta_n = \zeta_{|n|}$. We know that every quadratic number field is of the form $\mathbb{Q}[\sqrt{m}]$ for some squarefree integer m with $m \neq 0, 1$. Let's prime factorize $m = p_1 p_2 \cdots p_k$ where p_i are distinct primes since m is squarefree. (Note that we don't need a $\pm$ sign since p_i are allowed to be negative primes.) Recall that the discriminant of a quadratic number field is

$$\Delta_{\mathbb{Q}[\sqrt{m}]} = \begin{cases} 4m & m \equiv 2, 3 \mod 4 \\ m & m \equiv 1 \mod 4 \end{cases}$$

First suppose $m \equiv 1 \mod 4$. Then m can be factored as $m = (\ell_1 \cdots \ell_r)(p_1 q_1) \cdots (p_s q_s)$ where $p_j, q_j > 0$ are positive primes and ℓ_i are (possibly negative) primes satisfying $\ell_i \equiv 1 \mod 4$ and $p_j, q_j \equiv 3 \mod 4$. Then

$$\sqrt{m} = \left(\sqrt{\ell_1} \cdots \sqrt{\ell_r}\right) \left(\sqrt{-p_1}\sqrt{-q_1}\right) \cdots \left(\sqrt{-p_s}\sqrt{-q_s}\right).$$

Note that by (a), $\sqrt{\ell_i} \in \mathbb{Q}[\zeta_{\ell_i}]$ and $\sqrt{-p_j} \in \mathbb{Q}[\zeta_{p_j}]$. (resp q_j) Since $\mathbb{Q}[\zeta_a] \subset \mathbb{Q}[\zeta_b]$ for any $a \mid b$, it follows that $\sqrt{m} \in \mathbb{Q}[\zeta_m]$ since $\ell_i, p_j, q_j \mid m$. So any squarefree $m \equiv 1 \mod 4$ satisfies $\sqrt{m} \in \mathbb{Q}[\zeta_m] = \mathbb{Q}[\zeta_{\Delta_K}]$.

Next, suppose that $m \equiv 3 \mod 4$. This means that $m = pn$ where $p \equiv 3 \mod 4$ and $n \equiv 1 \mod n$ is some squarefree integer. There are now two cases. Without loss of generality, we can assume that $p = -1$ or p is a prime, since n can absorb all $1 \mod 4$ factors out of p. If $p = -1$, then $\sqrt{-1} \in \mathbb{Q}[\zeta_4]$ and by the earlier argument $\sqrt{n} \in \mathbb{Q}[\zeta_n]$. Combining this gives $\sqrt{n} = \sqrt{-1} \cdot \sqrt{n} \in \mathbb{Q}[\zeta_{4n}] = \mathbb{Q}[\zeta_{\Delta_K}]$ as desired. Now if p is a prime, then by (a) we know that $\sqrt{-p} \in \mathbb{Q}[\zeta_p]$, however since $\sqrt{-1} \in \mathbb{Q}[\zeta_4]$, we have $\sqrt{p} \in \mathbb{Q}[\zeta_p, \zeta_4] \subset \mathbb{Q}[\zeta_{4p}]$. Thus since $\sqrt{m} = \sqrt{p}\sqrt{n}$ we have $\sqrt{m} \in \mathbb{Q}[\zeta_{4pn}] = \mathbb{Q}[\zeta_{4m}] = \mathbb{Q}[\zeta_{\Delta_K}]$.

Our last case to consider is when $m \equiv 2 \mod 4$. Such m can be expressed as $m = 2n$ for some $n \equiv 1, 3 \mod 4$. By the results of the preceding paragraphs, $\sqrt{n} \in \mathbb{Q}[\zeta_{4n}]$. (If $n \equiv 1 \mod 4$, $\sqrt{n} \in \mathbb{Q}[\zeta_n] \subset \mathbb{Q}[\zeta_{4n}]$) Then by (b), $\sqrt{2} \in \mathbb{Q}[\zeta_8]$ so $\sqrt{m} = \sqrt{2}\sqrt{n} \in \mathbb{Q}[\zeta_{4 \cdot 2n}] = \mathbb{Q}[\zeta_K]$. This completes the proof.

Problem 3.8.

(a) Show that the ideal $(2, x)$ in $\mathbb{Z}[x]$ is not principal.

(b) Let $f, g \in \mathbb{Z}[x]$ and let m, n be the gcd's of the coefficients of f and g, respectively. Prove Gauss' Lemma: mn is the gcd of the coefficients of fg.

(c) Show that if $f \in \mathbb{Z}[x]$ and f is irreducible over $\mathbb{Z}$, then f is irreducible over $\mathbb{Q}$.

(d) Suppose f is irreducible over $\mathbb{Z}$ and the gcd of its coefficients is 1. Show that if $f \mid gh$ in $\mathbb{Z}[x]$, then $f \mid g$ or $f \mid h$.

(e) Show that $\mathbb{Z}[x]$ is a UFD, the irreducible elements being the polynomials f as in (d), along with the primes $p \in \mathbb{Z}$.

(a) Suppose for the sake of contradiction that $(2, x)$ is principal in $\mathbb{Z}[x]$. Then $(2, x) = (\alpha(x))$ for some $\alpha(x) \in \mathbb{Z}[x]$. Thus $2 = \alpha(x)\beta(x)$ for some $\beta(x)$, however this implies that $\alpha(x)$ has degree zero, and since 2 is prime it implies that $\alpha(x) = 1$ or 2. It clearly cannot be 1 since $1 \notin (2, x)$, so $\alpha(x) = 2$. But then $x = 2\beta(x)$ for some $\beta(x) \in \mathbb{Z}[x]$ which is impossible. So $(2, x)$ is not principal.

(b) Say a polynomial $f(x) \in \mathbb{Z}[x]$ is *primitive* if the gcd of its coefficients is 1. Clearly any polynomial $f(x) \in \mathbb{Z}[x]$ can be uniquely expressed as $f(x) = du(x)$ where d is the gcd of all of the coefficients of f and $u(x)$ is primitive. If we can prove that the product of two primitive polynomials is primitive, we'll have proved the claim since for $f, g \in \mathbb{Z}[x]$ and $f = d_1u_1$, $g = d_2u_2$ the product $fg = d_1d_2u_1u_2$ is the unique expression, so the gcd of fg is the product of the gcd of f and the gcd of g.

Now suppose f, g are primitive polynomials, and suppose for the sake of contradiction that $p \mid fg$ for some $d > 0$, assume without loss of generality that p is prime. Write $f(x) = a_0 + a_1x + \cdots + a_rx^r$ and $g(x) = b_0 + b_1x + \cdots + b_sx^s$. Let a_i be the the first coefficient of f not divisible by p and let b_j be the first coefficient of g not divisible by p. Then the coefficient of x^{i+j} in fg is of the form $a_0b^{i+j} + a_1b^{i+j-1} + \cdots + a^ib^j + \cdots + a_{i+j}b_0$. This must be divisible by p since it is a coefficient of fg, however every term except for a^ib^j is divisible by p. This is a contradiction so $p = 1$ and fg is primitive.

(c) Suppose f were reducible over $\mathbb{Q}$, say $f(x) = \frac{a}{b}\alpha(x)\beta(x)$ where $\alpha(x), \beta(x) \in \mathbb{Z}[x]$ are primitive and a, b are coprime. Then $bf(x) = a\alpha(x)\beta(x)$. The gcd of the left side is b and the gcd of the right side is a so $b = a$ and so $f(x) = \alpha(x)\beta(x)$. Thus $f(x)$ is reducible. This is the contrapositive of the required statement.

(d) Consider these as polynomials in $\mathbb{Q}[x]$. Then since $\mathbb{Q}[x]$ is a UFD we know that if $f \mid gh$ we have $f \mid g$ or $f \mid h$ in $\mathbb{Q}[x]$. Assume without loss of generality that $f \mid g$. This means that $g(x) = f(x)q(x)$ for some $q(x) \in \mathbb{Q}[x]$. We would like to show that $q(x) \in \mathbb{Z}[x]$ since this would imply that $f \mid g$ in $\mathbb{Z}[x]$. We can write $q(x) = \frac{a}{b}q'(x)$ for some $\frac{a}{b} \in \mathbb{Q}$ and primitive $q'(x) \in \mathbb{Z}[x]$. Then $g(x) = \frac{a}{b}f(x)q'(x)$. Since $f(x)q'(x)$ is primitive by (a), $\frac{a}{b}$ must be an integer, so $q(x) \in \mathbb{Z}[x]$ and we are done.

(e) Let $f(x) \in \mathbb{Z}[x]$ be some arbitrary polynomial. We can clearly decompose $f(x)$ into irreducibles $q_1(x) \cdots q_r(x)$. We can factor out the maximal $d \in \mathbb{Z}$ so that $f(x) = du_1(x) \cdots u_r(x)$ where the $u_i(x)$ are all primitive irreducibles. We can assume without loss of generality that the leading term of $u_i(x)$ are all positive. Then $f(x) = \pm p_1 \cdots p_s u_1(x) \cdots u_r(x)$ where $p_i \in \mathbb{Z}$ are positive primes. To prove uniqueness, suppose $f(x) = \pm q_1 \cdots q_{s'} w_1(x) \cdots w_{r'}(x)$ for some different primes and primitive irreducibles. Since $\pm p_1 \cdots p_s$ and $\pm q_1 \cdots q_{s'}$ are the gcd's of the coefficients of $f(x)$, we know that $p_1 \cdots p_s = q_1 \cdots q_{s'}$ so $s = s'$ and p_i and q_i are the same primes, just reordered because $\mathbb{Z}$ is a UFD. So $u_1(x) \cdots u_r(x) = w_1(x) \cdots w_{r'}(x)$. We know that $u_1(x) \mid w_1(x) \cdots w_{r'}(x)$ so by (d), $u_1(x) = w_i(x)$ for some i. Assume without loss of generality that $i = 1$ so $u_1(x) = w_1(x)$. Then by induction we can show that $r = r'$ and $u_i(x) = w_i(x)$. So the expression is unique up to some reordering of the primes.

Problem 3.11. Let K be a number field, and I a nonzero ideal in $\mathcal{O}_K$. Prove that $\|I\|$ divides $\mathrm{N}^K(\alpha)$ for all $\alpha \in I$, and equality holds iff $I = (\alpha)$.

Recall from Theorem 3.22c that we have $\|(\alpha)\| = \mathrm{N}^K(\alpha)$. Now for any $\alpha \in I$, we have $(\alpha) \subset I$, so by the third ring isomorphism theorem we have $\|I\| = |\mathcal{O}_K/I|$ divides $\|(\alpha)\| = \mathcal{O}_K/(\alpha)| = \mathrm{N}^K(\alpha)$, completing the proof.

Problem 3.12.

(a) Verify that $5S = (5, \alpha + 2)(5, \alpha^2 + 3\alpha - 1)$ in the ring $S = \mathbb{Z}[\sqrt[3]{2}], \alpha = \sqrt[3]{2}$.

(b) Show that there is a ring isomorphism

$$\mathbb{Z}[x]/(5, x^2 + 3x - 1) \to \mathbb{Z}_5[x]/(x^2 + 3x - 1).$$

(c) Show that there is a ring homomorphism

$$\mathbb{Z}[x]/(5, x^2 + 3x - 1) \to S/(5, \alpha^2 + 3\alpha - 1).$$

(d) Conclude that either $S/(5, \alpha^2 + 3\alpha - 1)$ is a field of order 25 or else $(5, \alpha^2 + 3\alpha - 1) = S$.

(e) Show that $(5, \alpha^2 + 3\alpha - 1) \neq S$ by considering (a).

(a) Note that $I = (5, \alpha+2)(5, \alpha^2+3\alpha-1) = (25, 5(\alpha+2), 5(\alpha^2+3\alpha-1), (\alpha+2)(\alpha^2+3\alpha-1))$. However $(\alpha + 2)(\alpha^2 + 3\alpha - 1) = 5\alpha^2 + 5\alpha$. So $5(\alpha + 1) \in I$ and $5(\alpha + 2) \in I$ so $5\alpha \in I$ and $5 \in I$. So $5S = I$ since $1 \notin I$.

(b) This is true by the third isomorphism theorem for rings; let $R = \mathbb{Z}[x]$, $J = (5)$, $I = (5, x^2 + 3x - 1)$. Then the third isomorphism theorem states that

$$\frac{R/J}{I/J} \cong \frac{R}{I}.$$

Note that $I/J = (5, x^2 + 3x - 1)/(5) = (x^2 + 3x - 1)\mathbb{Z}_5[x]$. Thus $\mathbb{Z}[x]/(5, x^2 + 3x - 1) \cong (\mathbb{Z}[x]/(5))/(x^2 + 3x - 1) = \mathbb{Z}_5[x]/(x^2 + 3x - 1)$.

(c) There is a surjective homomorphism $\varphi : \mathbb{Z}[x] \to S$ given by $f(x) \to f(\alpha)$. For any ideal $I \subset \mathbb{Z}[x]$, this induces a surjective homomorphism $\widetilde{\varphi} : \mathbb{Z}[x]/I \to S/\varphi(I)$ given by $f(x) + I \mapsto f(\alpha) + \varphi(I)$.

(d) First, note that $\mathbb{Z}_5[x]/(x^2+3x-1)$ is a field of 25 elements because x^2+3x-1 is irreducible in $\mathbb{Z}_5[x]$. Using the map from (c), we thus know that $\mathrm{Im}(\widetilde{\varphi}) = S/(5, \alpha^2 + 3\alpha - 1)$ is a finite field of size 25 or size 1. (Field homomorphisms can either be injective or the zero map.) If it's a finite field of size 25, we are done. Otherwise, $S/(5, \alpha^2 + 3\alpha - 1) = \{0\}$ so $(5, \alpha^2 + 3\alpha - 1)$.

(e) If $(5, \alpha^2 + 3\alpha - 1) = S$, then by (a) we have $5S = (5, \alpha + 2)S$ which is a contradiction because $\alpha + 2 \notin 5S$.

This means that (5) doesn't ramify in $\mathcal{O}_{\mathbb{Q}[\sqrt[3]{2}]}$. Checking LMFDB, we can actually see that $\mathcal{O}_{\mathbb{Q}[\sqrt[3]{2}]} = \mathbb{Z}[\sqrt[3]{2}]$. We also can show that $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}[\sqrt[3]{4}]$ and $\mathcal{O}_{\mathbb{Q}[\sqrt[3]{2}]} = \mathcal{O}_{\mathbb{Q}[\sqrt[3]{4}]}$, so (5) doesn't ramify in $\mathcal{O}_{\mathbb{Q}[\sqrt[3]{4}]}$ either.

Problem 3.16. Let $K \subset L$ be number fields. Denote by $G(\mathcal{O}_K)$ and $G(\mathcal{O}_L)$ the ideal class groups of K and L respectively.

(a) Show that there is a homomorphism $G(\mathcal{O}_L) \to G(\mathcal{O}_K)$ defined by sending $[I]$ to $[\mathrm{N}_K^L(I)]$.

(b) Let $\mathfrak{q}$ be a prime of $\mathcal{O}_L$ lying over a prime $\mathfrak{p}$ of $\mathcal{O}_K$. Let $d_\mathfrak{q}$ denote the order of the class containing $\mathfrak{q}$ in $G(\mathcal{O}_L)$, $d_\mathfrak{p}$ the order of the class containing $\mathfrak{p}$ in $G(\mathcal{O}_K)$. Prove that

$$d_\mathfrak{p} \mid d_\mathfrak{q} f(\mathfrak{q} \mid \mathfrak{p}).$$

(a) Recall that if $I \subset \mathcal{O}_L$, with prime factorization $I = \mathfrak{q}_1 \cdots \mathfrak{q}_n$, we define the norm of I as

$$\mathrm{N}_K^L(I) = \prod_{i=1}^{n} \mathfrak{p}_i^{f(\mathfrak{q}_i|\mathfrak{p}_i)}$$

where $\mathfrak{q}_i$ lies above the prime $\mathfrak{p}_i \subset \mathcal{O}_K$. Now let $\varphi : G(\mathcal{O}_L) \to G(\mathcal{O}_K)$ be the map defined in the problem. First we have to show that it is a well defined map, so suppose $I, J \subset \mathcal{O}_L$ and $I \sim J$ i.e. there are $\alpha, \beta \in \mathcal{O}_L$ such that $\alpha I = \beta J$. This is equivalent to saying that $(\alpha)I = (\beta)J$ so $\mathrm{N}_K^L(\alpha)\mathrm{N}_K^L(I) = \mathrm{N}_K^L(\beta)\mathrm{N}_K^L(J)$ so $\mathrm{N}_K^L(I) \sim \mathrm{N}_K^L(J)$. It's clearly a homomorphism because

$$\varphi([I][J]) = [\mathrm{N}_K^L(IJ)] = [\mathrm{N}_K^L(I)][\mathrm{N}_K^L(J)] = \varphi([I])\varphi([J]).$$

(b) Let $[\mathfrak{q}]$ be the class of $\mathfrak{q} \in G(\mathcal{O}_L)$ and $[\mathfrak{p}]$ be the class of $\mathfrak{p} \in G(\mathcal{O}_K)$. Then $\varphi([\mathfrak{q}]) = [\mathfrak{p}]^{f(\mathfrak{q}|\mathfrak{p})}$. By Lagrange's theorem, $[\mathfrak{q}]^{d_\mathfrak{q}} = e_{G(\mathcal{O}_L)}$ so $\varphi([\mathfrak{q}]^{d_\mathfrak{q}}) = [\mathfrak{p}]^{d_\mathfrak{q} f(\mathfrak{p}|\mathfrak{q})} = e_{\mathcal{O}_K}$. So again by Lagrange's theorem, we have $d_\mathfrak{p} \mid d_\mathfrak{q} f(\mathfrak{q} \mid \mathfrak{p})$ as desired.

Problem 3.19. Let $K \subset L$ be number fields. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$.

(a) Show that if $\alpha \in \mathcal{O}_L$ and $\beta \in \mathcal{O}_K$, and $\alpha\beta \in \mathfrak{p}\mathcal{O}_L$, then either $\alpha \in \mathfrak{p}\mathcal{O}_L$ or $\beta \in \mathfrak{p}$.

(b) Let $\alpha, \alpha_1, \ldots, \alpha_n \in \mathcal{O}_L$; $\beta, \beta_1, \ldots, \beta_n \in \mathcal{O}_K$, and $\alpha \notin \mathfrak{p}\mathcal{O}_L$. Suppose $\alpha\beta = \alpha_1\beta_1 + \cdots + \alpha_n\beta_n$. Prove that there exists $\gamma \in K$ such that $\beta\gamma$ and all of the $\beta_i\gamma$ are in $\mathcal{O}_K$ and the $\beta_i\gamma$ are not all in $\mathfrak{p}$.

(c) Prove the following generalization of Theorem 3.24: Let $\alpha_1, \ldots, \alpha_n$ be a basis for L over K consisting entirely of members of $\mathcal{O}_L$, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ which is ramified in $\mathcal{O}_L$. Then $\mathrm{disc}_K^L(\alpha_1, \ldots, \alpha_n) \in \mathfrak{p}$.

(a) Recall that $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a $K_\mathfrak{p}$-vector space, where $K_\mathfrak{q}$ is the residue field of $\mathfrak{q}$. Then if $\alpha\beta \in \mathfrak{p}\mathcal{O}_L$, this means that $\alpha\beta = 0 \in \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$, so by the properties of a vector space either $\alpha = 0 \in \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ or $\beta = 0 \in K_\mathfrak{p}$. These conditions are equivalent to $\alpha \in \mathfrak{p}\mathcal{O}_L$ and $\beta \in \mathfrak{p}$ as desired.

(b) We can assume that all of the β_i are in $\mathfrak{p}$ otherwise $\gamma = 1$ would work. Then since $\alpha\beta \in \mathfrak{p}\mathcal{O}_L$ yet $\alpha \notin \mathfrak{p}\mathcal{O}_L$ so by (a), $\beta \in \mathfrak{p}$. Recall the lemma from the proof of Theorem 3.22(b):

Lemma. Let A and B be nonzero ideals in a Dedekind domain R, with $B \subset A$ and $A \neq R$. Then there exists $\gamma \in K$ such that $\gamma B \subset R$, $\gamma B \not\subset A$.

Letting $A = \mathfrak{p}$ and $B = (\beta, \beta_1, \ldots, \beta_n)$ so that $B \subset A$, and $A \neq \mathcal{O}_K$ so we can apply the lemma to get a $\gamma \in K$ with $\gamma B \subset \mathcal{O}_K$ and $\gamma B \not\subset \mathfrak{p}$. Suppose for the sake of contradiction that $\gamma\beta_i \in \mathfrak{p}$.

Then $\gamma B \subset \mathfrak{p}$, so $\alpha(\gamma\beta) = \alpha_1(\gamma\beta_1) + \cdots + \alpha_n(\gamma\beta_n) \in \mathfrak{p}\mathcal{O}_L$. However $\alpha \notin \mathfrak{p}\mathcal{O}_L$, so $\gamma\beta \in \mathfrak{p}$ by (a). However $\gamma\beta \notin \mathfrak{p}$ since $\gamma B \not\subset \mathfrak{p}$. This is a contradiction, so one of the $\gamma\beta_i \in \mathfrak{p}$.

(c) Pick some prime $\mathfrak{q}$ lying over $\mathfrak{p}$ satisfying $e(\mathfrak{q} \mid \mathfrak{p}) > 1$. Then $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}I$ for some ideal $I \subset \mathcal{O}_L$. Finally, let's pick some $\alpha \in I - \mathfrak{p}\mathcal{O}_L$ so since $I \subset \mathfrak{q}$, α is in every prime of $\mathcal{O}_L$ lying over $\mathfrak{p}$ but $\alpha \notin \mathfrak{p}\mathcal{O}_L$. Write $\alpha = m_1\alpha_1 + \cdots + m_n\alpha_n$ for some $m_i \in K$. Then there is some $\beta \in \mathcal{O}_K$ such that $\beta m_i \in \mathcal{O}_K$. Then

$$\alpha\beta = (m_1\beta)\alpha_1 + (m_2\beta)\alpha_2 + \cdots + (m_n\beta)\alpha_n.$$

Then since $\alpha \notin \mathfrak{p}\mathcal{O}_L$, by (b) there is some $\gamma \in K$ such that $\beta\gamma$ and all of the $m_i\beta\gamma \in \mathcal{O}_K$ and the $m_i\beta\gamma$ are not all in $\mathfrak{p}$. Let $\kappa = \beta\gamma$ and $\kappa_i = m_i\beta\gamma$ so that

$$\alpha\kappa = \alpha_1\kappa_1 + \alpha_2\kappa_2 + \cdots + \alpha_n\kappa_n.$$

By definition, not all of the $\kappa_i \in \mathfrak{p}$, so say without loss of generality that $\kappa_1 \notin \mathfrak{p}$. Then by a set of column operation and using the fact that $\kappa_i \in \mathcal{O}_K$, we get

$$\mathrm{disc}_K^L(\alpha, \alpha_2, \ldots, \alpha_n) = \kappa_1^2 \mathrm{disc}_K^L(\alpha_1, \ldots, \alpha_n).$$

So since $\kappa_1 \notin \mathfrak{p}$, it suffices to show that $\mathrm{disc}_K^L(\alpha, \alpha_2, \ldots, \alpha_n) \in \mathfrak{p}$. Let M be some extension of L which is normal over K, and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of L in $\mathbb{C}$ fixing K. Recall that these can be extended to embeddings $\overline{\sigma_1}, \ldots, \overline{\sigma_n} : M \to \mathbb{C}$ which fix K and agree with σ_i on L. Let $\mathfrak{P}$ be some prime in $\mathcal{O}_M$ lying over $\mathfrak{p}$ with $e(\mathfrak{P} \mid \mathfrak{p}) > 1$. (Picking any prime lying over $\mathfrak{q}$ works) Then $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}J$ for some ideal $J \subset \mathfrak{P}$. We claim that $\overline{\sigma_i}(\alpha) \in \mathfrak{P}$ for all i. Note that $(\overline{\sigma_i})^{-1}(\mathfrak{P})$ is a prime of $\mathcal{O}_M$ lying over $\mathfrak{p}$, so $\alpha \in (\overline{\sigma_i})^{-1}(\mathfrak{P})$ and thus $\overline{\sigma_i}(\alpha) = \sigma_i(\alpha) \in \mathfrak{P}$. This implies that $\mathrm{disc}_K^L(\alpha, \alpha_2, \ldots, \alpha_n) \in \mathfrak{P}$. However since $\mathrm{disc}_K^L(\alpha, \alpha_2, \ldots, \alpha_n) \in \mathcal{O}_K$, it follows that $\mathrm{disc}_K^L(\alpha, \alpha_2, \ldots, \alpha_n) \in \mathfrak{p}$ since $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.