Mathematics W4043 Algebraic Number Theory
Assignment # 3

Benjamin Church

Worked With Matthew Lerner-Brecher

December 20, 2017

1. Let α be algebraic over $\mathbb{Q}$ with minimal polynomial:

$$P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 = (X - \alpha_1)\dots(X - \alpha_d)$$

Also, let $\alpha \in K$ with $[K : \mathbb{Q}(\alpha)] = m$. Then there must exist a basis of length m of K over $\mathbb{Q}(\alpha)$ which we write as $\{k_1, \dots, k_m\}$. Now, since $\{1, \alpha, \alpha^2, \dots, \alpha^{d-1}\}$ is a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ then an arbitrary element $k \in K$ can uniquely be wirtten as,

$$k = \sum_{i=1,j=0}^{m,d-1} k_i \alpha^j c_{ij}$$

for $c_{ij} \in \mathbb{Q}$. Thus, $\{k_1, k_1\alpha, \dots k_1\alpha^{d-1}, \dots, k_m\alpha^{d-1}\}$ is a basis for K. We express the transformation A_α in this basis. Now, $A_\alpha\left(d_i\alpha^j\right) = d_i\alpha^{j+1}$ but for any j, $\alpha^{j+1} \in \operatorname{span}\{1, \alpha, \dots, \alpha^{d-1}\}$ thus, $A_\alpha\left(d_i\alpha^j\right) \in \operatorname{span}\{d_i, d_i\alpha, \dots, d_i\alpha^{d-1}\}$ and therefore, so is A_α acting on any linear combination in $\operatorname{span}\{d_i, d_i\alpha, \dots, d_i\alpha^{d-1}\}$. So A_α acts invariantly on the subspace $\operatorname{span}\{d_i, d_i\alpha, \dots, d_i\alpha^{d-1}\}$ and thus is represented by a block diagonal matrix with m blocks of size $d \times d$. Also, each block has identical matrix elements because each $d_i \neq 0$ so,

$$A_\alpha\left(d_i\alpha^j\right) = d_i\alpha^{j+1} = \sum_{l=0}^{d-1} A_{lj} d_i \alpha^j \iff A_\alpha \alpha^j = \alpha^{j+1} = \sum_{l=0}^{d-1} A_{lj}\alpha^j$$

Thus, each block has identical matrix elements to A_α acting on $\mathbb{Q}(\alpha)$. Thus the trace of each block is $\alpha_1 + \cdots + \alpha_d$ and the determinant of each block is $\alpha_1 \cdots \alpha_d$. Since the trace of a block diagonal matrix is the sum of the traces of its blocks and likewise the determinant is the products of the block determinants, we conclude that:

$$\mathrm{Tr}_{\mathbb{Q}}^K(\alpha) = m(\alpha_1 + \cdots + \alpha_d) \quad \text{and} \quad \mathrm{N}_{\mathbb{Q}}^K(\alpha) = (\alpha_1 \cdots \alpha_d)^m$$

2. Let $K = \mathbb{Q}(\sqrt{-14})$ and because $-14 \equiv 2 \bmod 4$ we have that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$

   (a) $\mathrm{N}_{\mathbb{Q}}^K\left(3 + \sqrt{-14}\right) = 3^2 + 14 = 23$. If $3 + \sqrt{-14} = \alpha\beta$ with $\alpha, \beta \in \mathcal{O}_k$ then $\mathrm{N}_{\mathbb{Q}}^K\left(3 + \sqrt{-14}\right) = \mathrm{N}_{\mathbb{Q}}^K(\alpha)\,\mathrm{N}_{\mathbb{Q}}^K(\beta) = 23$ but 23 is prime so either $\mathrm{N}_{\mathbb{Q}}^K(\alpha) = 1$ or $\mathrm{N}_{\mathbb{Q}}^K(\beta) = 1$ thus one is a unit. Therefore, $3 + \sqrt{-14}$ is irreducible.

   (b) Suppose that for $x \in \mathcal{O}_K$ that $\mathrm{N}_{\mathbb{Q}}^K(x) = 3$ then $x = a + b\sqrt{-14}$ and $\mathrm{N}_{\mathbb{Q}}^K(x) = a^2 + 14b^2 = 3$ with $a, b \in \mathbb{Z}$. Since both terms are positive, $b > 0$ implies that $a^2 + 14b^2 \geq 14$ so we must have $b = 0$. Thus, $a^2 = 3$. However, 3 is square free so we reach a contradiction.

(c) $\mathrm{N}_{\mathbb{Q}}^{K}(3) = 3^2 = 9$ so if $\alpha\beta = 3$ for $\alpha, \beta \in \mathcal{O}_K$ then $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)\,\mathrm{N}_{\mathbb{Q}}^{K}(\beta) = 9$. Therefore, if neither is a unit (so neither has norm 1) then $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha) = \mathrm{N}_{\mathbb{Q}}^{K}(\beta) = 3$ which is impossible. Thus, 3 is irreducible.

(d) The ideal (3) is not prime because the product $(1+\sqrt{-14})\cdot(1-\sqrt{-14}) = 15 = 5\cdot 3 \in (3)$ however, $\mathrm{N}_{\mathbb{Q}}^{K}\left(1 \pm \sqrt{-14}\right) = 15$ which is not divisible by $\mathrm{N}_{\mathbb{Q}}^{K}(3) = 9$ so $1 \pm \sqrt{-14} \notin (3)$. I claim that $(3) = (3, 1+\sqrt{-14})(3, 1-\sqrt{-14})$ and that the ideals $(3, 1+\sqrt{-14})$ and $(3, 1-\sqrt{-14})$ are prime.

An arbitrary element of $(3, 1 \pm \sqrt{-14})$ is:

$$3x_1 + 3y_1\sqrt{-14} + (x_2 + y_2\sqrt{-14})(1 \pm \sqrt{-14}) = (3x_1 + x_2 \mp 14y_2) + (3y_1 + y_2 \pm x_2)\sqrt{-14}$$

Reducing the coeficients modulo 3,

$$3x_1 + 3y_1\sqrt{-14} + (x_2 + y_2\sqrt{-14})(1 \pm \sqrt{-14}) = (x_2 \pm y_2) + (y_2 \pm x_2)\sqrt{-14} \pmod 3$$

Since x_2 and y_2 are arbitary we can make any element of $\mathbb{F}_3$ subject to the constraints that the two terms are, in the plus case, congruent modulo 3, and in the minus case, congruent to minus eachother. By adding multiples of 3 to either component (which we can do because 3 is in both ideals) we recover any pair of coeficients subject to this constraint modulo 3.

Then, for $\alpha = a_1 + a_2\sqrt{-14} \in (3, 1+\sqrt{-14})$ and $\beta = b_1 + b_2\sqrt{-14} \in (3, 1-\sqrt{-14})$ take:

$$\alpha\beta = (a_1b_1 - 14a_2b_2) + (b_1a_2 + a_1b_2)\sqrt{-14} = (a_1b_1 + a_2b_1) + (b_1a_2 + a_1b_2)\sqrt{-14} \pmod 3$$

But $a_1 \equiv a_2 \bmod 3$ and $b_1 \equiv -b_2 \bmod 3$ so $a_1b_1 \equiv -a_2b_2 \bmod 3$ and $b_1a_2 \equiv -a_1b_2 \bmod 3$ thus $3 \mid \alpha\beta$ so $(3, 1+\sqrt{-14})(3, 1-\sqrt{-14}) \subset (3)$. Also,

$$3 = 3\cdot[3 - [1 - \sqrt{-14}]] + [1 + \sqrt{-14}]\cdot(-3) \in (3, 1+\sqrt{-14})(3, 1-\sqrt{-14})$$

Thus, $(3) \subset (3, 1+\sqrt{-14})(3, 1-\sqrt{-14})$ so $(3) = (3, 1+\sqrt{-14})(3, 1-\sqrt{-14})$.

It remains to show that these ideals are prime. If we add any disjoint element to $(3, 1 \pm \sqrt{-14})$ we are adding an element whose coeficients modulo 3 do not satisfy the above criteria (for the plus and minus cases seperately) i.e. if $\gamma = g_1 + g_2\sqrt{-14}$ and $g_1 \not\equiv \pm g_2 \bmod 3$ then $\gamma \mp g_2(1 \pm \sqrt{-14}) = (g_1 \mp g_2) \in (3, 1+\sqrt{-14}, \gamma)$ which is an integer that is non-zero modulo 3 and thus coprime to 3. By Bezout, there exist integers x, y such that $1 = 3x + (g_1 \mp g_2)y \in (3, 1+\sqrt{-14}, \gamma)$ and thus $(3, 1+\sqrt{-14}, \gamma) = \mathcal{O}_K$. Thus, adding any element to $(3, 1 \pm \sqrt{-14})$ gives the entire ring i.e. $(3, 1+\sqrt{-14})$ is maximal and thus prime.

3. Let $K = \mathbb{Q}(\sqrt{-d})$ for various values of d. Now,

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{-d}] & d \not\equiv -1 \bmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right] & d \equiv -1 \bmod 4 \end{cases}$$

i) Take $\alpha, \beta \in \mathcal{O}_K$ with $\beta \neq 0$ then, $\frac{\alpha}{\beta} \in K$ thus $\frac{\alpha}{\beta} = p + q\sqrt{-d}$ with $p, q \in \mathbb{Q}$.

In the case $d \not\equiv -1 \bmod 4$, take $n, k \in \mathbb{Z}$ to be the best integer approximations of p, q respectively i.e. $|p-n| \leq \frac{1}{2}$ and $|q-k| \leq \frac{1}{2}$. This is possible by Lemma 0.1. Now, define $\gamma = n + k\sqrt{-d} \in \mathcal{O}_K$ and $\delta = \alpha - \beta\gamma \in \mathcal{O}_K$. Thus,

$$\begin{aligned}
\mathrm{N}_{\mathbb{Q}}^{K}(\delta) &= \mathrm{N}_{\mathbb{Q}}^{K}(\beta)\,\mathrm{N}_{\mathbb{Q}}^{K}\left(\frac{\alpha}{\beta}-\gamma\right) = \mathrm{N}_{\mathbb{Q}}^{K}(\beta)\,\mathrm{N}_{\mathbb{Q}}^{K}\left((p-n)+(q-k)\sqrt{-d}\right) \\
&= \mathrm{N}_{\mathbb{Q}}^{K}(\beta)\cdot\left((p-n)^2+d(q-k)^2\right) \leq \mathrm{N}_{\mathbb{Q}}^{K}(\beta)\left(\frac{1}{4}+\frac{d}{4}\right) = \mathrm{N}_{\mathbb{Q}}^{K}(\beta)\,\frac{1+d}{4}
\end{aligned}$$

Therefore, if $d < 3$ then $\forall \alpha, \beta \in \mathcal{O}_K$ with $\beta \neq 0$ we have $\exists \gamma, \delta \in \mathcal{O}_K : \alpha = \beta\gamma + \delta$ and $\mathrm{N}_{\mathbb{Q}}^{K}(\delta) < \mathrm{N}_{\mathbb{Q}}^{K}(\beta)$ so $\mathcal{O}_K$ is Euclidean and thus a PID. These conditions holds for $d = 1, 2$.

In the case $d \equiv -1 \bmod 4$, take $k \in \mathbb{Z}$ to be the best integer approximations of $2q$ and n to be the best integer approximation of $p - \frac{k}{2}$ i.e. $|2q-k| \leq \frac{1}{2}$ and $|p-\frac{k}{2}-n| \leq \frac{1}{2}$. This is possible by Lemma 0.1. Now, define $\gamma = n + k\frac{1+\sqrt{-d}}{2} \in \mathcal{O}_K$ and $\delta = \alpha - \beta\gamma \in \mathcal{O}_K$. Thus,

$$\begin{aligned}
\mathrm{N}_{\mathbb{Q}}^{K}(\delta) &= \mathrm{N}_{\mathbb{Q}}^{K}(\beta)\,\mathrm{N}_{\mathbb{Q}}^{K}\left(\frac{\alpha}{\beta}-\gamma\right) = \mathrm{N}_{\mathbb{Q}}^{K}(\beta)\,\mathrm{N}_{\mathbb{Q}}^{K}\left(\left(p-n-\frac{k}{2}\right)+\left(q-\frac{k}{2}\right)\sqrt{-d}\right) \\
&= \mathrm{N}_{\mathbb{Q}}^{K}(\beta)\cdot\left(\left(p-n-\frac{k}{2}\right)^2+\frac{d}{4}(2q-k)^2\right) \leq \mathrm{N}_{\mathbb{Q}}^{K}(\beta)\left(\frac{1}{4}+\frac{d}{16}\right) = \mathrm{N}_{\mathbb{Q}}^{K}(\beta)\,\frac{4+d}{16}
\end{aligned}$$

Therefore, if $d < 12$ then $\forall \alpha, \beta \in \mathcal{O}_K$ with $\beta \neq 0$ we have $\exists \gamma, \delta \in \mathcal{O}_K : \alpha = \beta\gamma + \delta$ and $\mathrm{N}_{\mathbb{Q}}^{K}(\delta) < \mathrm{N}_{\mathbb{Q}}^{K}(\beta)$ so $\mathcal{O}_K$ is Euclidean and thus a PID. These conditions holds for $d = 3, 7, 11$.

ii) For $d = 19, 43, 67, 163$ the norm $\mathrm{N}_{\mathbb{Q}}^{K}\left(\frac{1+\sqrt{-d}}{2}\right) = \frac{1+19}{4} = 5, \frac{1+43}{4} = 11, \frac{1+67}{4} = 17, \frac{1+163}{4} = 41$ which are all prime. We are asked to establish that every prime $p \leq \mathrm{N}_{\mathbb{Q}}^{K}\left(\frac{1+\sqrt{-d}}{2}\right)$ is inert in $\mathcal{O}_K$. This is equivalent to $\left(\frac{-d}{p}\right) = -1$ which is equivalent to $\left(\frac{d}{p}\right) = -(-1)^{\frac{p-1}{2}}$. By quadratic reciprocity, $\left(\frac{p}{d}\right) = (-1)^{\frac{p-1}{2}\frac{d-1}{2}}\left(\frac{d}{p}\right)$ but every d in the list is 1 modulo 4 so $\left(\frac{p}{d}\right) = -1$. This must be checked for every prime $p < \frac{1+d}{4}$ which is tedious by hand but easily done with a computer and turns out to be true.

iii) Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ with $\mathrm{N}(\mathfrak{p}) < \frac{2\sqrt{d}}{\pi}$. Now, every non-zero ideal of $\mathcal{O}_K$ contains an elelment of $\mathbb{Z}^+$ (because for any $a \in I\setminus\{0\}$, $a\bar{a} \in I \cap \mathbb{Z}^+$). Let $z \in \mathfrak{p} \cap \mathbb{Z}^+$. By the fundamental theorem of arithmetic, $z = q_1^{k_1}\cdots q_n^{k_n}$ for primes $q_1, \ldots, q_n$. Thus, $\mathfrak{p} \supset (z) = (q_1)^{k_1}\cdots(q_n)^{k_n}$ so there exists and ideal I s.t. $\mathfrak{p}I = (q_1)^{k_1}\cdots(q_n)^{k_n}$ and thus by Dedekind unique prime factorization, $\mathfrak{p}$ must appear in the prime factorization of some (q_i). However, because K is a quadratic extension of $\mathbb{Q}$, one of $(q_i) = \mathfrak{p}\mathfrak{p}'$ or $(q_i) = \mathfrak{p}$ or $(q_i) = \mathfrak{p}^2$ must hold (since we established that $\mathfrak{p}$ is one of the factors and the factorization is unique). In all of these cases, $\mathrm{N}(\mathfrak{p}) = q_1$ or q_1^2 so $q_1 \leq \mathrm{N}(\mathfrak{p}_i) < \frac{2\sqrt{d}}{\pi} < \frac{1+d}{2}$. By part *(ii)* this implies that q_1 is inert i.e. $(q_1) = \mathfrak{p}$ so $\mathfrak{p}$ is principal. Now, consider any ideal I with $\mathrm{N}(I) < \frac{2\sqrt{d}}{\pi}$ then by Dedekind prime factorization, $I = \mathfrak{p}_1\cdots\mathfrak{p}_k$ and $\mathrm{N}(I) = \mathrm{N}(\mathfrak{p}_i)\cdots\mathrm{N}(\mathfrak{p}_k)$ so each $\mathfrak{p}_i$ has norm less than $\frac{2\sqrt{d}}{\pi}$ and thus is principal i.e. $\mathfrak{p}_i = (q_i)$. Therefore, $I = (q_1)\cdots(q_k) = (q_1\cdots q_k)$ so I is principal.

Now Corollary 5.10 states that every ideal class contains an ideal with norm less than Minkowski's constant $c_1 = (4/\pi)^{r_2} \frac{n!}{n^n} \sqrt{\Delta_K}$. In this case, the minimal polynomial of $\sqrt{-d}$ is $X^2 + d$ which has no real root and one pair of complex roots so $r_2 = 1$. Also, $\{1, \frac{1+\sqrt{-d}}{2}\}$ is a basis of $\mathcal{O}_K$ because $d \equiv -1 \bmod 4$ and the embeddings of K in $\mathbb{C}$ are $\mathrm{id} : x \mapsto x$ and $\sigma : x \mapsto \bar{x}$ thus

$$\Delta_K = \det \begin{pmatrix} 1 & \frac{1+\sqrt{-d}}{2} \\ 1 & \frac{1-\sqrt{-d}}{2} \end{pmatrix}^2 = d$$

Therefore, $c_1 = \frac{4}{\pi}\frac{2}{4}\sqrt{d} = \frac{2\sqrt{d}}{\pi}$. Thus each ideal class contains an ideal with norm less than $\frac{2\sqrt{d}}{\pi}$ which is therefore principal. Thus, by Lemma 0.2, every ideal class contains only principal ideals so $\mathcal{O}_K$ is a PID.

4. (a) Let $f \in \mathbb{Q}[X]$ have degree three and let $K/\mathbb{Q}$ be the splitting field of f with $[K : \mathbb{Q}] = 3$. Let $\sigma : K \to K$ denote the automorphism given by $\sigma(x) = \bar{x}$ which fixes $\mathbb{Q}$ so $\sigma \in Gal(K/\mathbb{Q})$. If for some $x \in K$, $\sigma(x) \neq x$ then $\sigma \neq \mathrm{id}_K$ so $\mathrm{ord}(\sigma) > 1$. However, $\sigma^2 = \mathrm{id}$ thus, $\mathrm{ord}(\sigma) = 2$ so $\langle \sigma \rangle$ is a subgroup of $Gal(K/\mathbb{Q})$ of order 2. However, because K is a splitting field, $K/\mathbb{Q}$ is Galois and thus $|Gal(K/\mathbb{Q})| = [K : \mathbb{Q}] = 3$. But then $|\langle \sigma \rangle| \not| \, |Gal(K/\mathbb{Q})|$ which contradicts Lagrange's Theorem. Thus, $\forall x \in K : \sigma(x) = x$. In paricular, because K is the splitting field of f, every root r of f is contained in K and thus satisfies $\sigma(r) = \bar{r} = r$ which means that r is real.

   (b) Consdier the polynomial $f(X) = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$. Let $\xi = \zeta + \zeta^6$ where ζ is a generator of the seventh roots of unity. Now, ξ is a root of f because,

$$\begin{aligned} &(\zeta + \zeta^6)^3 + (\zeta + \zeta^6)^2 - 2(\zeta + \zeta^6) - 1 = \\ &\zeta^3 + \zeta^4 + 3\zeta + 3\zeta^6 + \zeta^2 + 2 + \zeta^5 - 2(\zeta + \zeta^6) - 1 = \\ &1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 = 0 \end{aligned}$$

There are three such distinct choices: $\xi = \zeta_7 + \zeta_7^6,\ \zeta_7^2 + \zeta_7^5,\ \zeta_7^3 + \zeta_7^4$. Thus, these are the three roots of f. Furtheremore, $(\zeta_7 + \zeta_7^6)^2 - 2 = \zeta_7^2 + \zeta_7^5$ and $(\zeta_7 + \zeta_7^6)^3 - 3(\zeta_7 + \zeta_7^6) = \zeta_7^3 + \zeta_7^4$ and thus, $\zeta_7 + \zeta_7^6,\ \zeta_7^2 + \zeta_7^5,\ \zeta_7^3 + \zeta_7^4 \in \mathbb{Q}(\zeta_7 + \zeta_7^6)$. Therefore, $\mathbb{Q}(\zeta_7 + \zeta_7^6)$ is the splitting field of f. Since $\mathbb{Q}(\zeta_7 + \zeta_7^6)$ is extended by a single element, $[\mathbb{Q}(\zeta_7 + \zeta_7^6) : \mathbb{Q}] = 3$ because f is the minimal polynomial for $\zeta_7 + \zeta_7^6$ (because any f with $\zeta_7 + \zeta_7^6$ as a root must have at least three roots by the above) and f has degree three. Now, f has no roots in $\mathbb{F}_5$ because:

$$\begin{aligned} f(1) &= 1^3 + 1^2 - 2 \cdot 1 - 1 = 4 \pmod 5 \\ f(2) &= 2^3 + 2^2 - 2 \cdot 2 - 1 = 2 \pmod 5 \\ f(3) &= 3^3 + 3^2 - 2 \cdot 3 - 1 = 4 \pmod 5 \\ f(4) &= 4^3 + 4^2 - 2 \cdot 4 - 1 = 1 \pmod 5 \\ f(0) &= 0^3 + 0^2 - 2 \cdot 0 - 1 = 4 \pmod 5 \end{aligned}$$

Finally, consider the prime factorization of (5) in $\mathcal{O}_K$. $(5) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$. For each $\mathfrak{p}_i$, we have, $\xi + \mathfrak{p}_i \notin \mathbb{F}_5 \subset \mathcal{O}_K/\mathfrak{p}_i$. If this were true, then consider the map $\pi : \alpha \mapsto \mathfrak{p}_i + \alpha$ which is a ring homomorphism. Thus,

$$f(\pi(\xi)) = \pi(f(\xi)) = \pi(0) = 0_{\mathcal{O}_K/\mathfrak{p}_i}$$

Because the coeficients map into $\mathbb{F}_5$ if $\pi(\xi) \in \mathbb{F}_5$ then $f(\pi(\xi)) = 0$ which we know is impossible. Therefore, $\mathcal{O}_K/\mathfrak{p}_i \supset \mathbb{F}_5[\xi]$ but since f is irreducible over $\mathbb{F}_5$ (since it has degree 3 and no roots) we have $[\mathbb{F}_5[\xi] : \mathbb{F}_5] = 3$ and thus $[\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_5] \geq 3$ so $f_i \geq 3$. However,

$$\mathrm{N}(5) = \mathrm{N}_{\mathbb{Q}}^{K}(5) = 5^3$$

because 5 is fixed by all three galois automorphisms. Therefore,

$$3 = \sum_{i=1}^{k} e_i f_i$$

so the only possibility is that $k = 1$ with $e_1 = 1$ and $f_1 = 3$ (because each $f_i \geq 3$). This implies that there is exctly one prime factor with multiplicity one so (5) must itself be a prime ideal, $(5) = \mathfrak{p}$ i.e. 5 is inert in $\mathcal{O}_K$. Furthermore, the residue field at (5) is $\mathcal{O}_K/(5)$. The order of this residue field is $[\mathcal{O}_K : (5)] = \mathrm{N}(5\mathcal{O}_K) = \mathrm{N}_{\mathbb{Q}}^{K}(5) = 5^3 = 125$.

Lemmas

Lemma 0.1. *$\forall r \in \mathbb{R} : \exists z \in \mathbb{Z}$ s.t. $|z - r| \leq \frac{1}{2}$. In particular, this holds for $r \in \mathbb{Q}$.*

Proof. Consider $S = \{n \in \mathbb{Z} \mid r < n+1\}$. S is non-empty because $\mathbb{Z}$ is unbounded but S is bounded below by r so by well ordering, S has a least element z. Since $z \in S$, $r < z + 1$. Suppose that $r < z$ then $z - 1 \in S$ contradicting the fact that z is the least element. Thus, $z \leq r < z + 1$.

Now if $|r - z| < \frac{1}{2}$ then we are done. Else, $|r - z| = r - z \geq \frac{1}{2}$ so $1 - \frac{1}{2} \geq z + 1 - r$ so $(z + 1) - r \leq \frac{1}{2}$. However, $z + 1 > r$ so $|(z + 1) - r| \leq \frac{1}{2}$ and $z + 1 \in \mathbb{Z}$. $\square$

Lemma 0.2. *If an ideal class contains a principal ideal, then every ideal in the class is principal. Furthermore, the set of non-zero principal ideals is an ideal class.*

Proof. Let I be an ideal in the same class as (a). Then $I \sim (a)$ so there exist $\alpha, \beta \in \mathcal{O}_K$ s.t. $\alpha I = \beta(a)$. Thus, $\beta a \in \alpha I$ so for some $k \in I$, we have $\beta a = \alpha k$. Now for any $r \in I$ we have $\alpha r \in \beta(a)$ so $\alpha r = \beta s a$ for $s \in \mathcal{O}_K$. Thus, $\alpha r = \alpha k s$ so because $\mathcal{O}_K$ is a domain, $r = ks$ so $I \subset (k)$. But $k \in I$ so by closure and absorption, $(k) \subset I$. Thus, $I = (k)$ is principal. Also, $\alpha(\beta) = \beta(\alpha)$ so all non-zero principal ideals are equivalent. Thus, an ideal I is in the same class as (a) iff I is principal. $\square$