

MATH 6302 PSET 4

AUSTIN WU AND RISHI GUJJAR

Problem 1:**a:**

To begin we show addition

$$\sigma_k(r_1 + r_2) = (r_1 + r_2)(e^{(2k-1)\pi i/n}) = r_1 e^{(2k-1)\pi i/n} + r_2 e^{(2k-1)\pi i/n} = \sigma_k(r_1) + \sigma_k(r_2)$$

And also that multiplication holds

$$\sigma_k(r_1 r_2) = (r_1 r_2)(e^{(2k-1)\pi i/n}) = (r_1)(e^{(2k-1)\pi i/n}) \cdot (r_2)(e^{(2k-1)\pi i/n}) = \sigma_k(r_1) \cdot \sigma_k(r_2)$$

Note that this works since $e^{(2k-1)\pi i/n}$ is a root of $x^n + 1$ and since any multiple of $x^n + 1$ evaluates to 0 we have multiplicativity.

Now to show bijectivity,

Suppose $\exists r \in \mathbb{Z}[x]/(x^n + 1)$ s.t. $\sigma_k(r) = 0$ with $r(x) = r_0 + r_1 x + \dots + r_{n-1} x^{n-1}$. Then $\sigma_k(r) = r(e^{\pi i/n}) = 0$ but since if $p(e^{\pi i/n}) = 0$ for a integer polynomial p , then p is divisible by $x^n + 1$. Thus in $\mathbb{Z}[x]/(x^n + 1)$, $r(x) \equiv 0 \pmod{x^n + 1} \implies r = 0$. Thus since the kernel of σ_k is just 0 which implies injectivity.

Now also since any element in $\mathbb{Z}[e^{\pi i/n}]$ can be written as

$$r_0 + r_1 e^{\pi i/n} + \dots + r_m (e^{\pi i/n})^m$$

With $r_i \in \mathbb{Z}, m \in \mathbb{N}$. Thus since $e^{\pi i/n} = -1$ implies that every element in $\mathbb{Z}[e^{\pi i/n}]$ can be expressed as a linear combination of integer coefficients of the basis

$$1, e^{\pi i/n}, \dots, (e^{\pi i/n})^{n-1}$$

Now let $r(x) = r_0 + r_1 x + \dots + r_{n-1} x^{n-1} \in \mathbb{Z}[x]/(x^n + 1)$ represented by $\sigma_k(x) = (e^{(2k-1)\pi i/n})^m$ such that $(2k-1)m \equiv 1 \pmod{2n}$. Thus

$$\sigma_k(r(x^m)) = r_0 + r_1 e^{\pi i/n} + \dots + r_{n-1} (e^{\pi i/n})^{n-1}$$

Thus any element in $\mathbb{Z}[e^{\pi i/n}]$ is in the image of an $r \in \mathbb{Z}[x]/(x^n + 1)$ which implies surjectivity.

Thus since we have shown bijectivity, additivity, and multiplicativity which implies σ_k is a ring isomorphism. 

b:

For any ring homomorphism that maps to \mathbb{C}

$$\sigma^*(0) = \sigma^*(x)^n + \sigma^*(1)$$

Thus this implies that $\sigma^*(x)^n + 1 = 0$ since $\sigma^*(0) = 0, \sigma^*(1) = 1$ by definition of a ring homomorphism.

This implies that σ^* is a root in $x^n + 1 = 0$. Thus since there is a bound of n roots implies that there exists some $k \in [n]$ such that

$$\sigma^*(x) = e^{(2k-1)\pi i/n}$$

This implies that for any element $r \in \mathbb{Z}[x]/(x^n + 1)$ that

$$\sigma^*(r) = \sum_{i=0}^{n-1} r_i (\sigma^*(x))^i$$

and

$$\sigma_k(r) = \sum_{i=0}^{n-1} r_i (\sigma_k(x))^i$$

Finally since $\sigma_k(r) = \sigma^*(r)$ then they are equivalent



c:

Given $r \in \mathbb{Z}[x]/(x^n + 1)$, then

$$\|\sigma(r)\|^2 = \sum_{k=1}^n |\sigma_k(r)|^2 = \sum_{k=1}^n \sigma_k(r) \overline{\sigma_k(r)}$$

Now since $\sigma_k(r) = \sum_{i=0}^{n-1} r_i \omega_k^i$ and $\overline{\sigma_k(r)} = \sum_{j=0}^{n-1} r_j \omega_k^{-j}$ Then

$$\|\sigma(r)\|^2 = \sum_{k=1}^n \left(\sum_{i=0}^{n-1} r_i \omega_k^i \right) \left(\sum_{j=0}^{n-1} r_j \omega_k^{-j} \right) = \sum_{i,j=0}^{n-1} r_i r_j \sum_{k=1}^n \omega_k^{i-j}$$

But since $\omega_k = e^{(2k-1)\pi i/n}$ implies that there are $2n$ roots of unity where $\omega_k^n = -1$. This implies that $\sum_{k=1}^n \omega_k^m$ is equal to n if $m \equiv 0 \pmod{n}$ and 0 otherwise. Thus we can simplify our equation to be

$$\sum_{i,j=0}^{n-1} r_i r_j \sum_{k=1}^n \omega_k^{i-j} = n \sum_{i=0}^{n-1} r_i^2 = n \|r\|^2$$

and thus square rooting each side implies that

$$\|\sigma_k(r)\| = \sqrt{n} \|r\|$$



d:

Let $S = \sigma(r)$ for each $r \in \mathbb{Z}[x]/(x^n + 1) \subset \mathbb{C}^n$. Then for any $\sigma(r_1), \sigma(r_2) \in S$,

$$\sigma(r_1) + \sigma(r_2) = (\sigma_1(r_1) + \sigma_2(r_2), \dots, \sigma_n(r_1) + \sigma_n(r_2))$$

And since σ_k is a ring homomorphism implies

$$= \sigma(r_1 + r_2)$$

Similarly,

$$\sigma(r_1)\sigma(r_2) = (\sigma_1(r_1)\sigma_2(r_2), \dots, \sigma_n(r_1)\sigma_n(r_2))$$

And since σ_k is a ring homomorphism implies

$$= \sigma(r_1 r_2)$$

Now suppose there is a $r_1 r_2 = 0$. Then since \mathbb{C} has no zero divisors, $\forall k, \sigma_k(r_1) = 0$ or $\sigma_k(r_2) = 0$. But due to the fact that σ_k is injective in 1.1 so then $\sigma_k(r) = 0 \implies r = 0$. Thus S has no nontrivial zero divisors.

Define a map between the two as $z \in \sqrt{n}\mathbb{Z}^n$ as

$$A : z \mapsto (\sigma_1(z \frac{1}{\sqrt{n}}), \dots, \sigma_n(z \frac{1}{\sqrt{n}}))$$

Then this map is linear since we showed that σ_k is linear by definition. We also know this map is length preserving since

$$(\sigma_1(z \frac{1}{\sqrt{n}}), \dots, \sigma_n(z \frac{1}{\sqrt{n}})) = \|\sigma(z \frac{1}{\sqrt{n}})\| = \sqrt{n} \|z \frac{1}{\sqrt{n}}\| = \|z\|$$

Problem 2:**a:**

We claim that the explicit generator for \mathcal{I} is $s = 1$. Now let $r_1 = x, r_2 = -3x - 2$. Then

$$5r_1 + r_2(1+x) = 5x + (-3x-2)(1+x) = 5x - 3x - 3x^2 - 2 - 2x = -2 - 3x^2$$

But since we are working in $\mathbb{Z}[x]/(x^2+1)$ implies that $x^2 = -1$, so $-2 - 3x^2 = 3 - 2 = 1 = s$. Thus $s \in \mathcal{I}$. Now let $r_1 = 1 = s, r_2 = 0$. Thus $5 \cdot 1 + 0(1+x) = 5$. Now let $r_1 = 0, r_2 = 1 = s$. Thus $5 \cdot 0 + 1(1+x) = 1+x$. Thus we have shown $x+1$ and 5 are contained in the ideal generated by s . Thus we have shown both properties and \mathcal{I} is a principal ideal with explicit generator $s = 1$. 🧡

b:

Assume that it is a principal ideal. Then $\mathcal{I} = \{2r_1 + r_2(1+x)\}, r_1, r_2 \in R$. Then if it is principal there exists $s \in R$ such that $s = a + bx, a, b \in \mathbb{Z}$. So then if $I = (s)$, s divides every element in the ideal. This implies that s divides $2, 1+x$.

Now using multiplicative norms, let

$$N : R \rightarrow \mathbb{Z}, N(a + bx) = a^2 + 3b^2$$

Then the norms of the divisibility relations are

$$N(s) | N(2) = 4, N(s) | N(1+x) = 4$$

So $N(s) \in \{1, 2, 4\}$.

Now since $N(s) = 2$ is impossible since $a^2 + 3b^2 \equiv 0, 1 \pmod{3}$

Now since $N(s) = 4$ gives $b = 0, |a| = 2$ so $s = \pm 2$ but if $s = \pm 2$ then $\pm 2 | (1+x)$ implies $(1+x)/2 \in R$ which is not true. And if $|a| = |b| = 1$ then $s = \pm(1 \pm x)$ and $2 = sq, q$ being the quotient so $N(s)N(q) = 4 = 4N(q)$ so $N(q) = 1, q = \pm 1$. Thus $N(s) \neq 4$.

This means that $N(s)$ must be 1 which implies that $s = \pm 1$. This would imply that any common divisor of 2 and $1+x$ is a unit.

Now suppose $1 \in \mathcal{I}$. Then $\exists r_1, r_2 \in R$ s.t. $1 = 2r_1 + r_2(1+x)$. But since every element of $R = \mathbb{Z}[x]/(x^2+3)$ can be uniquely written as $a + bx, a, b \in \mathbb{Z}$ then let $r_1 = a + bx, r_2 = c + dx$ implies that

$$1 = 2a + 2bx + c + dx + cx + dx^2$$

So then since $x^2 = -3$ in R , $dx^2 = -3d$. Thus


$$1 = (2a + c - 2d) + x(2b + c + d)$$

This gives a system of two equations

$$1 = 2a + c - 3d$$


$$2b + c + d = 0$$

And since they have the same parity both of these equations cannot satisfy, hence a contradiction. and $1 \notin \mathcal{I}$.

Now since we showed that if $I = (s)$ was principal that its generator is a common divisor of 2 and $1 + x$ so $s = \pm 1$ and $\mathcal{I} = R$ but $\mathcal{I} \neq R$ so we have a contradiction. Thus it is not a principle ideal. 

c:

Now since if n is a power of two the polynomial $x^n + 1$ becomes irreducible implies that there are no factors over \mathbb{Z} . This then implies that the quotient ring $R = \mathbb{Z}[x]/(x^n + 1)$ does not contain a zero divisor.

Now since $s_1 R = s_2 R$ implies that s_1 divides s_2 $s_2 = us_1$ and that s_2 divides s_1 $s_1 = vs_2$. This implies that $s_1 = v(us_1) = (vu)s_1$ by associativity. Thus $s_1(1 - vu) = 0$. But since since the integral domain does not contain a zero divisor and $s_1 \neq 0$ then $1 - vu = 0 \implies vu = 1$ which implies that $v = u^{-1}$ and $u^{-1}u = 1$. 

Problem 3:**a:**

Recall that a hexagonal lattice can be represented with a basis of

$$\begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \sqrt{3}/2 \end{bmatrix}$$

Then $\|b_1\| = 1 = \lambda_1(\mathcal{L})$ and so $\Pi_2(b_2) = \begin{bmatrix} 0 \\ \frac{\sqrt{3}}{2} \end{bmatrix}$ which is the shortest vector in $\Pi_2(\mathcal{L})$.

Thus it is a HKZ reduced basis. So doing gram schmidt on it we trivially get that $\|\tilde{b}_1\| = \left\| \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\| = 1$ and then

$$\|\tilde{b}_2\| = \|\Pi_{b_1^\perp}(b_2)\| = \left\| \begin{bmatrix} 0 \\ \frac{\sqrt{3}}{2} \end{bmatrix} \right\| = \frac{\sqrt{3}}{2}$$

So then

$$\frac{\|\tilde{b}_1\|}{\|\tilde{b}_2\|} = \frac{1}{\sqrt{3}/2} = \frac{2}{\sqrt{3}}$$

b:

Recall that minkowski's theorem states

$$\lambda_1(\mathcal{L}) \leq \sqrt{\gamma_j} \text{vol}(L)^{\frac{1}{j}}$$

Now given j , consider the j dimensional sublattice $\mathcal{L}' = \Pi_{n-k+1}(\mathcal{L})$. Thus

$$\text{vol}(\mathcal{L}') = \Pi_{k=1}^j \|\tilde{b}_{n-j+k}\|$$

and $\lambda_1(\mathcal{L}') = \|\tilde{b}_{n-j+1}\|$ by the definition of a HKZ reduced basis. We also know that $\gamma_j \leq j \forall j$. This implies that

$$\|\tilde{b}_{n-j+1}\| \leq \sqrt{j} (\Pi_{k=1}^j \|\tilde{b}_{n-j+k}\|)^{\frac{1}{j}}$$

So raising everything by j , dividing by $\|\tilde{b}_{n-j+1}\|$, and rearranging indices implies that

$$\|\tilde{b}_{n-j+1}\|^{j-1} \leq j^{j/2} \Pi_{k=1}^{j-1} \|\tilde{b}_{n-k+1}\|$$

Thus this implies that

$$\|\tilde{b}_{n-j+1}\| \leq j^{j/(2(j-1))} \Pi_{k=1}^{j-1} \|\tilde{b}_{n-k+1}\|^{1/(j-1)}$$

And so squaring everything implies that

$$\|\tilde{b}_{n-j+1}\|^2 \leq j^{j/(j-1)} \Pi_{k=1}^{j-1} \|\tilde{b}_{n-k+1}\|^{2/(j-1)}$$



c:

To begin, let's prove the base case of $j = 2$.

$$\begin{aligned} \|\tilde{b}_{n-2+1}\|^2 &\leq 2^{2/1} \Pi_{k=1}^1 \\ \|\tilde{b}_{n-k+1}\|^2 &\implies \|\tilde{b}_{n-1}\|^2 \leq 4\|\tilde{b}_n\|^2 \end{aligned}$$

And since Question 3.1 implies that $\frac{\|\tilde{b}_n\|}{\|\tilde{b}_{n-1}\|} = \sqrt{3}/2 \leq 2 \leq \sqrt{4}$ implies that this is true. Thus the $j = 2$ base case holds. Now to induct over j . Suppose this holds at j . Then to induct over j assume

$$\|\tilde{b}_{n-j+1}\|^2 \leq j(\Pi_{k=2}^j k^{1/(k-1)}) \|\tilde{b}_n\|^2$$

is true. Then by equation 1

$$\begin{aligned} \|\tilde{b}_{n-j}\| &\leq (j+1)^{(j+1)/j} \Pi_{k=1}^j \|\tilde{b}_{n-k+1}\|^{2/(j)} \\ &= (j+1)^{1+1/j} (\|\tilde{b}_{n-j+1}\|^{2/j} \prod_{i=1}^{j-1} \|\tilde{b}_{n-i+1}\|^{2/j}) \end{aligned}$$

So by applying the inductive hypothesis to each term we get

$$\leq (j+1)^{1+1/j} \left(\left(j \prod_{k=2}^j k^{1/(k-1)} \|\tilde{b}_n\|^2 \right)^{2/j} \prod_{i=1}^{j-1} \left((j-i+1) \prod_{k=2}^{j-i+1} k^{1/(k-1)} \|\tilde{b}_n\|^2 \right)^{2/j} \right)$$

Which implies that by simplifying evaluating the nested $\Pi_{k=2}^r k^{1/(k-1)}$ terms and applying an exponent of $2/j$ with rearranging we get

$$= (j+1) \left(\prod_{k=2}^{j+1} k^{1/(k-1)} \right) \|\tilde{b}_n\|^2$$

Thus by mathematical induction this holds

**d:**

Recall that since

$$\begin{aligned} \|\tilde{b}_{n-j+1}\|^2 &\leq j \cdot (\Pi_{k=2}^j k^{1/(k-1)}) \cdot \|\tilde{b}_n\|^2 \implies \\ \frac{\|\tilde{b}_{n-j+1}\|^2}{\|\tilde{b}_n\|^2} &\leq j \cdot (\Pi_{k=2}^j k^{1/(k-1)}) \end{aligned}$$

Now since $2 \leq k \leq j \leq n$ since k is always greater than 1 and its exponent is greater than 0 we know that $k^{1/(k-1)} \leq n^{1/(k-1)} \forall 2 \leq k \leq n$. Thus

$$j \cdot (\Pi_{k=2}^j k^{1/(k-1)}) \leq j \cdot (\Pi_{k=2}^j n^{1/(k-1)}) \leq n \cdot (\Pi_{k=2}^j n^{1/(k-1)}) = n \cdot (n^{\sum_{k=2}^j 1/(k-1)})$$

And using the fact about harmonic numbers $H_n := \sum_{i=1}^n 1/i \implies H_n \leq \log(n) + 1$ implies that

$$n \cdot (n^{\sum_{k=2}^j 1/(k-1)}) \leq n \cdot (n^{\log(j)+1})$$

And since we know that $\log(j) \leq \log(n) \forall 2 \leq j \leq n$,

$$n \cdot (n^{\log(j)+1}) \leq n \cdot (n^{\log(n)+1}) = n^{\log(n)+2}$$

Thus we have shown that

$$\frac{||\tilde{b}_{n-j+1}||^2}{||\tilde{b}_n||^2} \leq n^{\log(n)+2}$$

Now since we have shown it for any possible j implies that

$$\max_{1 \leq j \leq n} \frac{||\tilde{b}_{n-j+1}||^2}{||\tilde{b}_n||^2} \leq n^{\log(n)+2}$$

e:

Given (b_1, \dots, b_i) , $||b_1||$ is still equal to $\lambda_1(\mathcal{L})$. Similarly, for any $k \in \{1, \dots, i\}$, $(\Pi_k(b_k), \dots, \Pi_k(b_i))$ is still an HKZ reduced basis since $(\Pi_k(b_k), \dots, \Pi_k(b_n))$ is a HKZ reduced basis.

Thus both axioms of a HKZ reduced basis still satisfy.

Now given

$$\omega(B) = \max_{j \geq i} \frac{||\tilde{b}_i||}{||\tilde{b}_j||}$$

Implies that since

$$\max_{1 \leq j \leq n} \frac{||\tilde{b}_{n-j+1}||^2}{||\tilde{b}_n||^2} \leq n^{\log(n)+2}$$

That $\omega(B) \leq \sqrt{n^{\log(n)+2}} = n^{\log(n)/2+1}$



Problem 4:

A like 20 hours