THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Tutorial 10 Solutions
8th April 2024

- If you have any questions, please contact Eddie Lam via echlam@math.cuhk.edu.hk or in person during office hours.

1. (a) The norm function $|a+bi| = a^2+b^2$ is the square of length/modulus of $a+bi$ when regarded as a complex number. It is clear that if $0 \neq |w| \leq |z|$, it is clear that there exists at least one of $\{w, iw, -w, -iw\}$ such that one of $\{z+w, z+iw, z-w, z-iw\}$ has strictly smaller norm than z, let $z+\epsilon w$ be that number, where $\epsilon = \pm 1$ or $\pm\, i$. This process may be continued if $|w| \leq |z+\epsilon w|$. However, since $|z|$ is finite, this process will terminate at finite step, meaning that there exists $k = a+bi \in \mathbb{Z}[i]$ such that $|z-(a+bi)w| < |w|$. Taking $r = z - kw$, we obtained the desired claim.

   (b) Let $I \subset \mathbb{Z}[i]$ be an ideal, let d be an element in I such that $|d|$ attains the minimum, i.e. $|d| = \min\{|x| : x \in I\}$. We will show that $I = (d)$. It is trivial that $(d) \subset I$, since $d \in I$. For the other inclusion, let $x \in I$, by division theorem (part (a)), we have $x = kd + r$ for some $k, r \in \mathbb{Z}[i]$ such that $|r| < |d|$. Since $r = x - kd \in I$, if $r \neq 0$, it would contradict minimality assumption of d. Therefore, $x = kd \in (d)$.

2. No, the ideal $(2, x) \subset \mathbb{Z}[x]$ is not principal. Note that $(2, x) = \{\sum_{i=0}^{n} a_i x^i : n \in \mathbb{N}, a_0 \in 2\mathbb{Z}, a_1, ..., a_n \in \mathbb{Z}\}$. If $(2, x) = (f(x))$, then either $f(x)$ is constant polynomial or having degree at least 1. In the first case where $f(x)$ is constant, $f(x)$ must be equal to 2, then $x \notin (2)$. Otherwise, $f(x)$ is a polynomial of degree at least 1, then clearly $2 \notin (f(x))$ since the degree of constant polynomial 2 is strictly smaller. Either case led to a contradiction, so it was false that $(2, x)$ is a principal ideal.

3. Let $I = (1+i)$, consider the ring homomorphism $\mathbb{Z} \to \mathbb{Z}[i]/(1+i)$ by $\varphi(1) = 1 + I$. We have to show that this homomorphism is surjective and the kernel is given by $2\mathbb{Z}$. For surjectivity, note that since $1 + i \in I$, we have $i + I = -1 + i$, therefore we may write $a + bi + I = a - b + I = \varphi(a - b)$, thus showing surjectivity.

   It is clear that $2 \in I$ since $2 = (1+i)(1-i)$, therefore $\varphi(2) = 0 + I$ and so $2\mathbb{Z} \subset \ker\varphi$. Note that $\varphi(1) = 1 + I$ is not equal to $0 + I$ (otherwise $|1| = 1 < |1+i| = 2$ would imply that $1 + i$ is not a generator of the ideal). Therefore $2\mathbb{Z} = \ker\varphi \subsetneq \mathbb{Z}$.

   By first isomorphism theorem, we obtain the desired result.

4. Assuming the result of Q5c, we have $\mathbb{Z}[i]/(2) \cong \mathbb{Z}_2[x]/(x^2+1)$. Now the polynomial $x^2+1 = x^2-1 = (x-1)(x+1) = (x+1)^2$ in $\mathbb{Z}_2[x]$, since $1 = -1$ in that ring. Therefore, we may write $\mathbb{Z}_2[x]/(x^2+1) = \mathbb{Z}_2[x]/((x+1)^2) = \mathbb{Z}_2[x+1]/((x+1)^2) \cong \mathbb{Z}_2[y]/(y^2)$ by setting $y = x + 1$.

   One can also formally prove the statement using first isomorphism theorem. Write $I = (2)$. Inspired by the above, it is natural to define $\varphi : \mathbb{Z}_2[y] \to \mathbb{Z}[i]/(2)$ by $\varphi(y) = 1+i+I$ (since $y = x + 1$ and x corresponds to i uner the isomorphism $\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i]$.) This is a well-defined homomorphism since $2 + I = (1 + I) + (1 + I) = \varphi(1) + \varphi(1) = \varphi(0) = 0 + I$. It remains to prove that φ is surjective and has kernel given by (y^2).

Let $a+bi+I$ be any element in $\mathbb{Z}[i]/(2)$, then because $\varphi(y)=1+i$ and $\varphi(1)=1$, we have $a+bi+I=\varphi((a-b)+by)$, this proves surjectivity of φ.

It is also clear that $(y^2)\subset\ker\varphi$, since $\varphi(y^2)=(1+i)^2+I=2i+I=0+I$ since $2i\in I$. Conversely, let $p(y)\in\ker\varphi$, we may write $p(y)=a_0+a_1y+y^2\sum_{j=2}^N a_jy^{j-2}$. Then $\varphi(p(y))=a_0+a_1\varphi(y)+\cancelto{0}{\varphi(y^2)}\sum_{j=2}^N a_j\varphi(y^{j-2})+I=a_0+a_1\varphi(y)+I=a_0+a_1+a_1i+I=0+I$. This implies that $(a_0+a_1)+a_1i\in(2)$ is a multiple of 2, so both a_0,a_1 are even integers in $\mathbb{Z}_2$, i.e. 0. Thus we have shown that any polynomial $p(y)\in\ker\varphi$ can be expressed as $y^2\sum_{j=2}^N a_jy^{j-2}\in(y^2)$.

By first isomorphism theorem, we obtained the desired result.

5. (a) We will prove in general that for a prime number of $\mathbb{Z}$, the quotient ring $\mathbb{Z}[i]/(p)$ is finite of order p^2. Write $I=(p)$, it is possible to show that any element $a+bi+I\in\mathbb{Z}[i]/(p)$ is equal to one of the following $\{x+yi+(p):0\le x,y<p-1\}$, and these elements are distinct. Let $a+bi+(p)$, by performing division algorithm on a,b, we obtain remainders $a-k_1p=x$ and $b-k_2p=y$ so that $0\le x,y<p-1$, clearly $(a+bi)-(x+yi)=p(k_1+k_2i)\in(p)$, so they represent the same class $a+bi+I=x+yi+I$. The elements of $\{x+yi+(p):0\le x,y<p-1\}$ are all distinct because otherwise, p would divide a nonzero integer smaller than p, which is absurd.

   (b) By part (a), there are 9 elements in $\mathbb{Z}[i]/(3)$, represented by $0,1,2,i,1+i,2+i,2i,1+2i,2+2i$. Write $I=(3)$. Note that we may write $(a+bi+I)(a-bi+I)=a^2+b^2+I$. Also note that, $a^2+b^2\in I$ precisely when $a,b\in I$, this is simply because $1^2=1$ and $2^2=4$ is equal to 1 modulo I. Since $1+I$ and $2+I$ are both their own inverses, this shows that for $a+bi+I\neq0+I$, a^2+b^2+I is equal to $1+I$ or $2+I$, which is always invertible. Thus we have $(a+bi+I)(a-bi+I)(a^2+b^2+I)^{-1}=1+I$. This shows that any nonzero element in $\mathbb{Z}[i]/(3)$ is invertible, so it is a field.

   As for $\mathbb{Z}[i]/(5)$, we may find explicity zero divisors in the ring. This is due to the fact that 5 is reducible in $\mathbb{Z}[i]$, explicitly $5=(2+i)(2-i)$. Therefore $(2+i+(5))(2-i+(5))=5+(5)=0+(5)$. So it cannot be a field.

   (c) For the first isomorphism, we may consider the ring homomorphism $\varphi:\mathbb{Z}[x]\to\mathbb{Z}[i]/(p)$ by $\varphi(x)=i$. This homomorphism is in fact the composition $\mathrm{ev}_i:\mathbb{Z}[x]\to\mathbb{Z}[i]$ where $\mathrm{ev}_i(f(x))=f(i)$ and $\pi:\mathbb{Z}[i]\to\mathbb{Z}[i]/(p)$ the canonical projection map. Since both ev_i and π are surjective, so is their composition. And we have

$$\begin{aligned}
\ker\varphi=\ker(\pi\circ\mathrm{ev}_i)&=\{f(x)\in\mathbb{Z}[x]:\ \pi(\mathrm{ev}_i(f)=0\}\\
&=\{f(x)\in\mathbb{Z}[x]:\ \mathrm{ev}_i(f)\in\ker\pi\}\\
&=\mathrm{ev}_i^{-1}(\ker\pi)\\
&=\mathrm{ev}_i^{-1}((p))\\
&=\{f(x)\in\mathbb{Z}[x]:\ f(i)=p\cdot(a+bi)\}\\
&=\{f(x)\in\mathbb{Z}[x]:\ (f-pg)(i)=0\text{ for some }g\in\mathbb{Z}[x]\}\\
&=\{f(x)\in\mathbb{Z}[x]:\ f(x)-pg(x)=(x^2+1)h(x)\}\\
&=(p,x^2+1).
\end{aligned}$$

   This proves that $\mathbb{Z}[x]/(p,x^2+1)\cong\mathbb{Z}[i]/(p)$ by first isomorphism theorem.

The other one is obtained similarly, by considering a homomorphism $\psi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]/(x^2+1)$, which is given by a composition $r_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ and $\pi : \mathbb{Z}_p[x] \to \mathbb{Z}_p[x]/(x^2+1)$. Again, both maps are quotient maps (the map r_p sends $f(x)$ to $\overline{f(x)}$ where the coefficients are taken to be mod p) so they are surjective, and it suffices to compute the kernel.

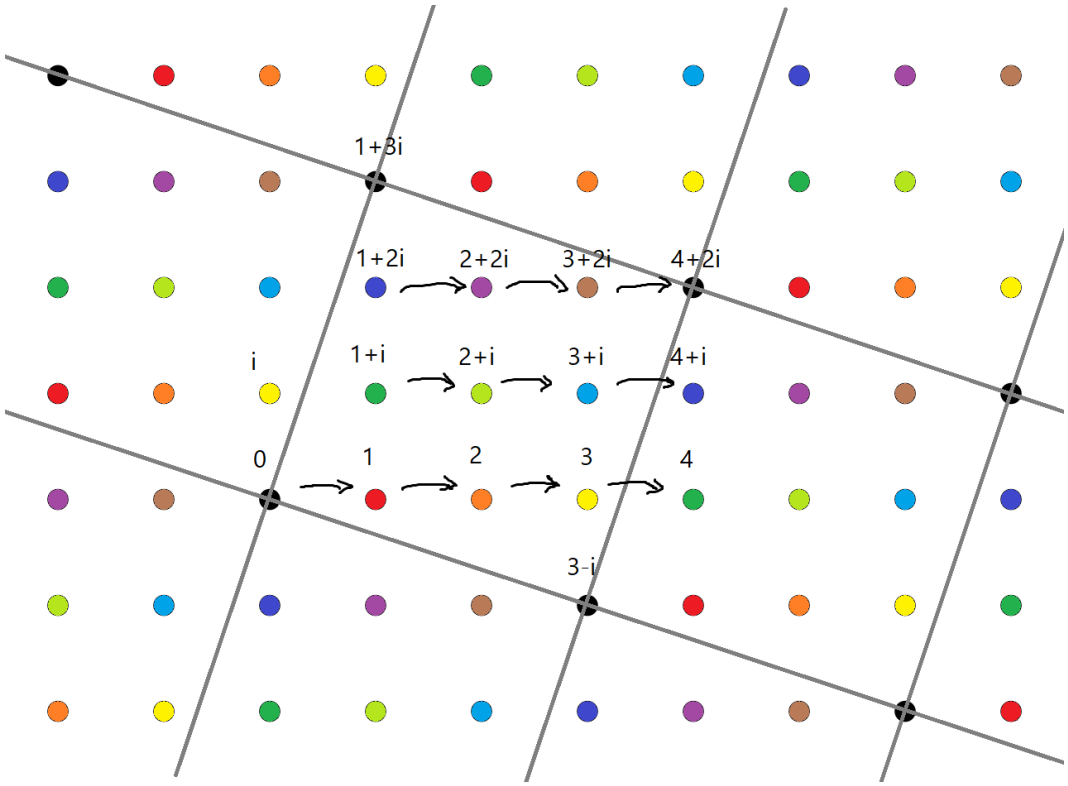
$$\begin{aligned}
\ker \psi = \ker(\pi \circ r_p) &= \{f(x) \in \mathbb{Z}[x] : \pi(r_p(f)) = 0\} \\
&= r_p^{-1}(\ker \pi) \\
&= r_p^{-1}((x^2+1)) \\
&= \{f(x) \in \mathbb{Z}[x] : \overline{f(x)} = (x^2+1) \cdot g(x)\} \\
&= \{f(x) \in \mathbb{Z}[x] : f(x) - (x^2+1)g(x) = ph(x)\} \\
&= (p, x^2+1).
\end{aligned}$$

Here in the second last equality, we are identifying $\mathbb{Z}[x] \to \mathbb{Z}_p[x] \cong \mathbb{Z}[x]/(p)$. Meaning that $f(x)$ and $(x^2+1)g(x)$ are equal in $\mathbb{Z}_p[x]$ if and only if they differ by a multiple of p, when regarded as polynomials over $\mathbb{Z}[x]$. This implies that $\mathbb{Z}[x]/(p, x^2+1) \cong \mathbb{Z}_p[x]/(x^2+1)$.

Long remark: The series of preceding exercise should highlight the difficulty in the study of $\mathbb{Z}[i]/(a+bi)$ in general. For example, when $a+bi = p$ is an ordinary prime number of $\mathbb{Z}$, then the quotient $\mathbb{Z}[x]/(p)$ depends on whether p can be written as a product of non-unit elements in $\mathbb{Z}[i]$, i.e whether p is irreducible in $\mathbb{Z}[i]$. It turns out that such p precisely corresponds the prime numbers that can be expressed as a sum of two squares. There is a remarkable theorem dating back to Fermat that describes the prime numbers $p \in \mathbb{Z}$ that can be expressed as sum of two squares, these are exactly the primes whose remainder modulo 4 is 1. For example, $5 \equiv 1$ modulo 4, and it can be expressed as a sum $1^2 + 2^2$. Therefore, it is reducible in $\mathbb{Z}[i]$ since $5 = 1^2 + 2^2 = (1+2i)(1-2i)$. On the other hand, 3 is not equivalent to 1 modulo 4, and it cannot be expressed as sum of two squares, and it is irreducible in $\mathbb{Z}[i]$, so the quotient ring is a field (of order 9), which gives an example of a finite field not of the form $\mathbb{Z}/p\mathbb{Z}$.

In the case when $\gcd(a, b) = 1$, we in fact do have a clean description of $\mathbb{Z}[i]/(a+bi)$, it is isomorphic to $\mathbb{Z}/(a^2+b^2)\mathbb{Z}$. This can be proven rather directly, using methods described in the lecture and tutorial. One simply consider the homomorphism $\mathbb{Z} \to \mathbb{Z}[i]/(a+bi)$. Then the coprime condition guarantees the surjectivity: there are $x, y \in \mathbb{Z}$ so that $ax + by = 1$, therefore $(a+bi)(y+xi) = (ay - bx) + (ax + by)i = k + i$ and we have $i + I = -k + I$.

The case when a, b are not necessarily coprime is more complicated, it can be solved using a generalization of the Chinese remainder theorem, and factorization of a Gaussian integers into irreducibles. Nonetheless, there is a nice geometric picture that allows one to gain intuitions on the structure of $\mathbb{Z}[i]/(a+bi)$, at least revealing the underlying additive group structure. One may think of $\mathbb{Z}[i]$ as a lattice in the complex plane $\mathbb{C}$, that means that $(\mathbb{Z}[i], +) \cong \mathbb{Z} \times i\mathbb{Z} \cong \mathbb{Z}^2$ as abelian groups. Then the underlying additive subgroup structure of any ideal $(a+bi) \subset \mathbb{Z}[i]$ is a sublattice, i.e. $(a+bi) = \{(a+bi) \cdot (x+yi) : x+yi \in \mathbb{Z}[i]\} = (a+bi)\mathbb{Z} \times i(a+bi)\mathbb{Z} \subset \mathbb{Z}^2$. Using, the example of $\mathbb{Z}[i]/(1+3i)$ again, we have the following diagram.



The dots are elements in $\mathbb{Z}[i]$. The larger square lattice (the black dots) is the ideal $(1+3i)$. Dots with the same color represent the same element in the quotient $\mathbb{Z}[i]/(1+3i)$. The red dot is the multiplicative identity $1+(1+3i)$, which happens to be a generator of the additive group structure of quotient ring, as depicted by the black arrow. When the element "escapes" the "fundamental parallelogram", i.e. the square with its elements labelled, it is equivalent to the element in original one after a translation by elements in $(1+3i)$. For example, $3+1=4$ represents the same element as $1+i$. And one can see the cyclic structure pictorial from this diagram.

Homework for you: Try to see for yourself what happens when we consider $\mathbb{Z}[i]/(p)$ where $p \in \mathbb{Z}$ is an integer prime, and compare $\mathbb{Z}[i]/(1+i)$ and $\mathbb{Z}[i]/(2+2i)$.

6. For a cubic polynomial, it is reducible if and only if it has a root. This is because if a cubic is reducible, it will factor into a linear term times a quadratic term, or a product of three linear terms. In either case, there will be a root corresponding to the linear term. Thus, it suffices to check: $f(0)=1$, $f(1)=4$, $f(2)=3$, $f(3)=4$ and $f(4)=3$; and $g(0)=2$, $g(1)=2$, $g(2)=1$, $g(3)=1$ and $g(4)=4$. So both polynomials are irreducible.

7. (a) If $f(x)=x^4+kx^2+1$ is reducible in $\mathbb{Z}[x]$, suppose that it has a linear factor $x-a$, i.e. $f(a)=0$. Then by $f(x)=f(-x)$, we also have $f(-a)=0$. Therefore $x+a$ is also a factor. So $f(x)=(x^2-a^2)(x^2+cx+d)=x^4+cx^3+(d-a^2)x^2+a^2cx-a^2d$. Looking at degree 3 coefficients gives $c=0$. And $-a^2d=1$, which implies that $a=\pm 1$ and $d=-1$. In this case, $f(x)=(x^2-1)(x^2-1)=(x^2+2x+1)(x^2-2x+1)$.

   Assume now that $f(x)$ does not have irreducible linear factor, then it must be a product of irreducible quadratic factors $f(x)=(x^2+ax+b)(x^2+cx+d)=x^4+(a+c)x^3+(ac+b+d)x^2+(ad+bc)x+bd$. By considering degree 3 coefficients, we obtain $c=-a$ immediately. So that $f(x)=x^4+(-a^2+b+d)x^2+a(d-b)x+bd$.

Since the constant term $bd = 1$, this implies that $b = d = 1$ or $b = d = -1$. Therefore, $f(x) = x^4 + (2b - a^2)x^2 + 1$. And we have $k = 2b - a^2 = \pm 2 - a^2$. The irreducible factors are $x^2 + ax + b$ and $x^2 - ax + b$, where $b = \pm 1$.

(b) The first statement follows from part (a), from the previous argument, if $f(x)$ has linear factors, then $f(x) = (x^2 - 1)(x^2 - 1) = (x^2 + 2x + 1)(x^2 - 2x + 1) = x^4 - 2x^2 + 1$, so we have $a = 0, b = -1$ or $a = -2, b = 1$. In either case, $k = -2 = 2b - a^2$.

If $f(x)$ is reducible and does not have linear factors, then this case was already explained in part (a), we necessarily have $k = 2b - a^2$.

(c) If $f(x) = x^4 - 22x^2 + 1$ was reducible, then $-22 = \pm 2 - a^2$, i.e. $a^2 = 20$ or $a^2 = -24$, both are impossible since $a \in \mathbb{Z}$. Therefore f must be irreducible.

(d) $f(x) = x^4 - 23x^2 + 1$ is reducible since $f(x) = (x^2 - 5x + 1)(x^2 + 5x + 1)$.