Name: Huize Shi - A92122910
Discussion: A04
Homework: 3

---

1. (a) Show that $\mathbb{Z}[w] = \{a + bw \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$ where $w = \frac{-1+\sqrt{-3}}{2}$

Addition:

$$\begin{aligned}
&\left(a + b\left(\frac{-1+\sqrt{-3}}{2}\right)\right) - \left(c + d\left(\frac{-1+\sqrt{-3}}{2}\right)\right) \\
&= \left((a-c) + (b+d)\left(\frac{-1+\sqrt{-3}}{2}\right)\right)
\end{aligned}$$

Multiplication:

$$\begin{aligned}
&\left(a + b\left(\frac{-1+\sqrt{-3}}{2}\right)\right) \cdot \left(c + d\left(\frac{-1+\sqrt{-3}}{2}\right)\right) \\
&= ac + (ad+bc)\left(\frac{-1+\sqrt{-3}}{2}\right) + bd\left(\frac{-1+\sqrt{-3}}{2}\right)^2 \\
&= (ac - \frac{ad}{2} - \frac{bc}{2} - \frac{bd}{2}) + (ad+bc+bd)\frac{\sqrt{-3}}{2} \\
&= ac - (ad+bc+bd)\frac{1}{2} + (ad+bc+bd)\frac{\sqrt{-3}}{2} \\
&= ac + (ad+bc+bd)\frac{-1+\sqrt{-3}}{2}
\end{aligned}$$

Hence shown $\mathbb{Z}[w]$ is a subring of $\mathbb{C}$.

(b) Show that the field of fraction of $\mathbb{Z}[w]$ is $\mathbb{Q}[w] = \{a + bw \mid a, b \in \mathbb{Q}\}$.

Multiplicative inverse (field): From part a, we can use similar process to show that $\mathbb{Q}$ is a subring of $\mathbb{C}$. Show there is multiplicative inverses. Let $\hat{w} = \frac{-1-\sqrt{-3}}{2}$

$$\begin{aligned}
\frac{1}{a+bw} &= \frac{a+b\hat{w}}{(a+bw)(a+b\hat{w})} \\
&= \frac{a+b\hat{w}}{a^2-ab+b^2}
\end{aligned}$$

$$\begin{aligned}
(a+bw)\frac{a+b\hat{w}}{a^2-ab+b^2} &= \frac{a^2-ab+b^2}{a^2-ab+b^2} \\
&= 1
\end{aligned}$$

Hence we found the inverse of the general term $a + bw$ is therefore $\frac{a+b\hat{w}}{a^2-ab+b^2}$.

Ring homomorphism:

$$\theta : \mathbb{Z}[w] \mapsto \mathbb{Q}[w]$$
$$\theta(x) = x$$

The homomorphism property of identity mapping is trivial. Given a generic element in $\mathbb{Q}[w]$, show it is of the form $\theta(x)\theta(x)^{-1}$.

$$\begin{aligned}\frac{a}{b} + \frac{c}{d}w &= \frac{ad + bcw}{bd} \\ &= \theta(ad + bcw)\theta(bd)^{-1}\end{aligned}$$

2. (a) Prove that $< u >= R$ iff $u \in \mathcal{U}$
   By definition, $< u >= \{ru \mid r \in R\}$. Since R is a unital commutative ring, $1_R \in \{ru \mid r \in R\}$. Assume towards contrary, u is not a unit, this means $ru \neq 1_R$. This is a contradiction, hence u must be a unit.

   (b) Suppose D is an integral domain. Prove that $< a >=< b > \Leftrightarrow \exists u \in \mathcal{U}(D) \mid a = bu$
   Since both a, b generated the set, we can represent any element in the set as bu or au' This means the following holds:

$$\begin{aligned}a &= bu \\ b^{-1}aa^{-1} &= b^{-1}bua^{-1} \\ b^{-1} &= ua^{-1} \\ b &= u^{-1}a \\ b &= au' \\ u^{-1}a &= au' \\ a^{-1}a &= u'u \\ u'u &= 1\end{aligned}$$

   Hence shown $\exists u \in \mathcal{U}(D) \mid a = bu$.

3. Given R_1 and R_2 are unital commutative rings, and $I \lhd R_1 \times R_2$. Prove that $I = I_1 \times I_2$.

$$\begin{aligned}(x_1, x_2) &\in I \\ (x_1, x_2) \cdot (r_1, r_2) &\in I \\ (x_1, x_2) \cdot (r_1, r_2) &= (x_1r_1, x_2r_2) \\ x_1r_1 &\in I_1 \\ x_2r_2 &\in I_2 \\ (x_1r_1, x_2r_2) &= I_1 \times I_2 \\ I &= I_1 \times I_2\end{aligned}$$

4. Prove that $< 2, x > \lhd \mathbb{Z}[x]$ is not a principal ideal.

Constant polynomial: Assume $< f(x) >$ is constant polynomial, the generated set contains the polynomials with even coefficient (multiple of 2).

Degree 1: Assume $< f(x) >$ is polynomial of degree at least 1, the generated set contains only polynomial with no even constant term including 2.
Hence shown $< f(x) > \neq < 2, x >$.

5. (a) Find the remainder of 102459087 divided by 9:

$$\begin{aligned} 102459087 &\overset{9}{\equiv} 1+0+2+4+5+9+0+8+7 \\ &\overset{9}{\equiv} 36 \overset{9}{\equiv} 0 \end{aligned}$$

(b) Find the remainder of 102459087 divided by 11:

$$\begin{aligned} 102459087 &\overset{11}{\equiv} 1-0+2-4+5-9+0-8+7 \\ &\overset{11}{\equiv} -6 \overset{11}{\equiv} 5 \end{aligned}$$

(c)

6.

$$\begin{aligned} \hat{a} &\overset{5}{\equiv} a \\ \hat{b} &\overset{5}{\equiv} b \\ f(a+bi) &= \hat{a} \oplus 2\hat{b} \\ &\overset{5}{\equiv} \hat{a} + 2\hat{b} \\ &\overset{5}{\equiv} a + 2b \end{aligned}$$

(a) Proove homomorphism:

Addition:

$$\begin{aligned} & f((a+bi)+(c+di)) \\ &= f((a+c)+(b+d)i) \\ &= (a \hat{+} c) + 2(b \hat{+} d) \\ &\overset{5}{\equiv} (a+c) + 2(b+d) \\ &\overset{5}{\equiv} (a+2b) + (c+2d) \\ &= \hat{a} + 2\hat{b} + \hat{c} + 2\hat{d} \\ &= f(a+bi) + f(c+di) \end{aligned}$$

Multiplication:

$$
\begin{aligned}
&f((a+bi)\cdot(c+di))\\
&= f(ac-bd+(ad+cb)i)\\
&= (ac \mathbin{\hat{-}} bd) + 2(ad \mathbin{\hat{+}} cb)\\
&\overset{5}{\equiv} (ac-bd)+2(ad+cb)\\
&\overset{5}{\equiv} (a+2b)\cdot(c+2d)\\
&f(a+bi)\cdot f(c+di)
\end{aligned}
$$

(b) Show that $< -2+i > \subseteq ker\ f$
$f(-2+i) = -2+2 = 0$. $-2+i$ is in kernel of f. This means the set generated by $-2+i$ is also in kernel of f.