HW9

1. Prove the followings.

- **(1). Give an example of integral domain s.t. dose not satisfy the factor chain condition.**
- **(2). Let R be a integral domain satisfying factor chain condition. Prove R is a UFD iff any two elements in R have greatest common divisor.**

Proof. i) Let $R=\overline{\mathbb{Z}}$ be the integral closure of $\mathbb{Z}$ in C . In other words, R consists of every complex number that is the root of a nonzero monic polynomial in $Z[x]$ (And yes, R is a ring, for an elegant proof of why integral closures are rings, check out Kaplansky's book Commutative Rings). Note that every element of Q$\backslash\mathbb{Z}$ is not in R (eg there is no monic polynomial in $\mathbb{Z}[x]$ with $\frac{1}{2}$ as a root), thus R is not a field. So, pick any nonzero nonunit $r\in R$. Then, there exist $a_0,a_1,\cdots,a_{n-1}\in\mathbb{Z}$ (not all zero) such that

$$a_0+a_1r+a_2r^2+\cdots+a_{n-1}r^{n-1}+r^n=0$$

Note that $\sqrt{r}$ is a complex number and in fact

$$a_0+a_1(\sqrt{r})^2+a_3(\sqrt{r})^6+\cdots+a_{n-1}(\sqrt{r})^{2n-2}+(\sqrt{r})^{2n}=0$$

Therefore $\sqrt{r}\in R$ and we have $r=\sqrt{r}\sqrt{r}$. Thus no nonzero nonunit element of R is irreducible and in fact R is an antimatter domain.

ii) One direction is easy. 设 R 是 UFD, $a,b\in R$, $a=up_1^{e_1}\cdots p_t^{e_t}$, $b=vp_1^{f_1}\cdots p_t^{f_t}$, 其中 $u,v\in R^\times,p_i$ 为素元素, $e_i,f_i\geq 0(\forall i)$, 则 $(a,b)=\prod_{i=1}^t p_i^{\min\{e_i,f_i\}}$.

反之, 设 p 为 R 的不可约元, $p\mid ab(a,b\in R)$. 若 $(p,a)=p$, 则 $p\mid a$. 否则 (由于 p 不可约) 可设 $(p,a)=1$.

由此易见 $(pb,ab)=b$: 设 $(pb,ab)=d$,则 $b\mid d$. 设 $d=ub$, 只要证 $u\in R^\times$. 事实上, 由于 $d\mid pb$, 故存在 $e\in R$ 使得 $pb=de$, 即 $pb=ube$, 亦即 $p=ue$, 所以 $u\mid p$. 同样地, 存在 $f\in R$使得 $ab=df$, 即 $ab=ubf$, 亦即 $a=uf$, 所以 $u\mid a$. 于是 $u\mid(p,a)$. 而 $(p,a)=1$, 故 $u\in R^\times$. 由于 $p\mid ab$, 故 $p\mid(pb,ab)=b$.

这就证明了 p 为 R的素元素, 于是 R 是 UFD. □

2. Prove the followings.

- **(1). Let R be a UFD, S is a multiplicatively closed set of** $\mathrm{R},0\notin S$**. Prove that the ring of fractions** $S^{-1}R$ **is a UFD.**
- **(2). Give an example to show that the subring of a UFD may not a UFD.**
- **(3). Let R be a UFD, P is a prime ideal of R . Give an example to show that the quotient ring** R/P **may not a UFD.**

Proof.

3. 提示: 设 $\frac{r}{s}, \frac{r'}{s'} \in S^{-1}R$, 由于 s, s' 都是 $S^{-1}R$ 的可逆元，故 (r, r') 是 $\frac{r}{s}, \frac{r'}{s'}$ 的最大公因子. 再应用习题 2 的结果.

4. 提示: $R = \mathbb{Z}[\sqrt{-5}]$ 不是 UFD, 它是其分式域 (当然是 UFD) 的子环.

5. 提示: $\mathbb{Z}[x]$ 是 UFD, (x^2+5) 是其素理想，但 $\mathbb{Z}[x]/(x^2+5) \cong \mathbb{Z}[\sqrt{-5}]$ 不是 UFD.

□

3. (1). Prove that any principle ideal of $\mathbb{Z}[x]$ is not a maximal ideal. (2). Prove that all non-zero prime ideals in PID are maximal ideals.

Proof. i) For any principle ideal $(f(x)) \subseteq \mathbb{Z}[x]$, $R \neq (f(x), x) \supseteq (f(x))$ if $f(0) = 0$. If $f(0) \neq 0$, choose prime $p \nmid a_n$ where a_n is the leading coefficient of f. Then $(f(x), p) \neq R$.

Alternating proof. Let $p \in \mathbb{Z}$ be a prime such that $p \nmid \mathrm{LC}(f)$, where $\mathrm{LC}(f)$ stands for the leading coefficient of f. Moreover p is non-zero in $\mathbb{Z}[x]/(f)$, hence invertible in $\mathbb{Z}[x]/(f)$, so there are $g, h \in \mathbb{Z}[x]$ such that $pg(x) + f(x)h(x) = 1$. It follows that $\bar{f}\bar{h} = \bar{1}$ in $(\mathbb{Z}/p\mathbb{Z})[x]$, and this is impossible since $\deg \bar{f} = \deg f \geq 1$.

ii) Let I be a prime ideal of $\mathbb{Z}[x]$, then $I = (a)$ where a is a prime and so a is irreducible. If there is $(a) \subsetneq (b) \neq R$, then $a = mb$ for some m. Either m or b is invertible, and both of them is impossible. □

4. Let K be a field. The formal power series $\sum_{i=0}^{\infty} a_i x^i$ $(a_i \in K)$ form a ring under the usual addition and multiplication, which is called the ring of formal power series in one variable over K , denoted by $K[[x]]$.

- **(1). Let $f(x) = \sum_{i=0}^{\infty} a_i x^i \in K[[x]]$, prove that $f(x)$ is invertible iff $a_0 \neq 0$.**
- **(2). Prove $K[[x]]$ is a PID.**

Proof. i) Note that $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$, then $f(x) = a_0 + g(x)$ and $f(x)^{-1} = \frac{1}{a_0} \sum_{n=0}^{\infty} (-g(x)/a_0)^n \in K[[x]]$. If $a_0 = 0$, then for any $g \in K[[x]]$, $gf(0) = 0$ and so f is not invertible.

ii) If $a_0 = 0$, then f is invertible and $(f) = K[[x]]$. Let $I \neq K[\![x]\!]$ be an ideal of $K[[x]]$, then $f \in I$ yields that $a_0 = 0$. It follows that $I = (x)$. Therefore, $I \in \{(x), K[\![x]\!], (0)\}$ and so $K[\![x]\!]$ is a PID. □

5. Let R be a PID, $a, b, d \in R$, then $(a, b) = (d)$ (as ideals) iff d is the greatest common divisor of a and b.

Proof. If $(a, b) = (d)$, then $d \mid a$ and $d \mid b$. If $e \mid a$ and $e \mid b$, then $(e) \supseteq (a, b) = (d)$ and so $e \mid d$. Thus d is the gcd.

Conversely if d is the greatest common divisor of a and b, then $(a, b) \subseteq (d)$. If there exists $(a, b) = (e) \subsetneq (d)$, then $d \mid e$ and $a \mid e$, $a \mid e$, which is impossible. Therefore, $(a, b) = (d)$. □

6. Let D, R be PIDs, $R \subseteq D. a, b, d \in R, d$ is the greatest common divisor of a and b in R. Prove that d is also the greatest common divisor of a and b in D.

Proof. Note that $d \mid a$ and $d \mid b$ hold in D. It follows that $(a, b) \subseteq (d)$ in D. Since d is the greatest common divisor of a, b in R, we have $(a, b) = (d)$ in R. There exists $r_1, r_2 \in R$ such that $r_1 a + r_2 b = d$ and it also holds in D. Therefore, $(a, b) \supseteq (d)$ in D and so $(a, b) = d$. That is, d is also the greatest common divisor of a and b in D. □

7. Let K be a algebraic number field. We call $\alpha \in K$ an algebraic integer if α is a root of a monic polynomial with integer coefficients. Let d be integer with no square factors. Let $K = \mathbb{Q}(\sqrt{d})$.

- **(1). If $d \equiv 2, 3(\mod 4)$, prove that all algebraic integer in K is a set:**

$$\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

- **(2). If $d \equiv 1(\mod 4)$, prove that all algebraic integer in K is a set:**

$$\left\{a + b\frac{1+\sqrt{d}}{2} \middle| a, b \in \mathbb{Z}\right\}$$

Therefore all algebraic integers in K form a ring, called the algebraic integer ring of K.

Proof. i) If $a + b\sqrt{d}$ is an algebraic integer, then $x^2 - 2ax + a^2 - b^2 d \in \mathbb{Z}[x]$, that is, $2a$ and $a^2 - b^2 d$ are integers. Assume that one of $a, b \notin \mathbb{Z}$. If $a = k/2$ with odd k, then $4 \mid k^2 - 4b^2 d$ and $4b^2 d \equiv 1 \pmod 4$, which is impossible by $4b^2 \equiv 1 \pmod 4$. If $a \in \mathbb{Z}$, then $b^2 d \in \mathbb{Z}$ and $b \in \mathbb{Z}$ by d square-free, contradiction. Now we finish the proof.

ii) Similarly, $2a$ and $a^2 - b^2 d$ are integers. Assume that one of $a, b \notin \mathbb{Z}$. If $a = k/2$ with odd k, then $4 \mid k^2 - 4b^2 d$ and $4b^2 d \equiv 1 \pmod 4$ yield that $b = m/2$ with odd m. Therefore, $a + b\sqrt{d} = k/2 + m/2\sqrt{d}$. If $a \in \mathbb{Z}$, then $b \in \mathbb{Z}$. Hence, $a + b\sqrt{d} \in \left\{a + b\frac{1+\sqrt{d}}{2} \middle| a, b \in \mathbb{Z}\right\}$. □

8. (1). Prove the algebraic integer ring of $\mathbb{Q}(\sqrt{-3})$ is a ED. (2). Prove the algebraic integer ring of $\mathbb{Q}(\sqrt{2})$ is a ED. (3). Prove the algebraic integer ring of $\mathbb{Q}(\sqrt{5})$ is a ED.

Proof. i) 这是课本的做法：

例 2.12 令 $R = \mathbb{Z}[\mathrm{i}] = \{m + n\mathrm{i} \mid m, n \in \mathbb{Z}\}$, 其中 $\mathrm{i} = \sqrt{-1}$. 我们来证明 R 是欧几里得环. 为此，对于 $a = m + n\mathrm{i} \in R$, 定义 $d(a) = |a|^2 = m^2 + n^2$. 对于任意的 $a, b \in R$, $b \neq 0$, $bR = \{(m + n\mathrm{i})b \mid m, n \in \mathbb{Z}\}$ 是复平面 $\mathbb{C}$ 上边长为 $|b|$ 的正方形网格的格点. 设与点 a 距离最近的格点为 $(m_0 + n_0\mathrm{i})b$. 取 $q = m_0 + n_0\mathrm{i}$, $r = a - qb$, 则 $|r| < |b|$ (即正方形上一点到四个顶点距离的最小值小于边长), 故 $d(r) < d(b)$. 这就证明了 R 是欧几里得环.

Similarly, 用锐角为$\pi/3$的菱形代替正方形。In this case, $d(m + n\frac{1+\sqrt{-3}}{2}) = m^2 + mn + n^2$.

ii) $a + b\sqrt{2} \mapsto |a^2 - 2b^2|$. It is similar as the following property.

Recall

$\mathbb{Z}[\sqrt{-2}]$ **is an Euclidean domain.**

Proof. Define $r: \mathbb{Q}[\sqrt{-2}] \to \mathbb{Q}, a+b\sqrt{-2} \mapsto a^2+2b^2$ and note that $r(\mathbb{Z}[\sqrt{-2}]) \subseteq \mathbb{Z}$, $r(a)r(b) = r(ab)$ for all $a, b \in \mathbb{Q}[\sqrt{2}]$. For any $a+b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ and $c+d\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$, we aim to find $q \in \mathbb{Z}\sqrt{-2}$ such that $r(a+b\sqrt{2} - q(c+d\sqrt{2})) < r(c+d\sqrt{2})$, that is, $r(\frac{a+b\sqrt{2}}{c+d\sqrt{2}} - q) < 1$.

It suffices to show for any $u+v\sqrt{-2} \in \mathbb{Q}\sqrt{-2}$ there exists $m+n\sqrt{-2} \in \mathbb{Z}\sqrt{-2}$ satisfying $|(u-m)^2 - 2(v-n)^2| < 1$, and we only need to choose $m, n \in \mathbb{Z}$ such that $|u-m| < 1/2$ and $|v-n| < 1/2$ as $1 \cdot 1/4 + 2 \cdot 1/4 < 1$. □

iii) Take

$$\begin{aligned} \delta : \mathbb{Z} + \frac{1+\sqrt{5}}{2}\mathbb{Z} &\to \mathbb{Z}, \\ a + b\frac{1+\sqrt{5}}{2} &\mapsto \left| \left(a + b\frac{1+\sqrt{5}}{2}\right)\left(a + b\frac{1-\sqrt{5}}{2}\right) \right|. \end{aligned}$$

Now we finish the proof. □

Remark. In fact, i) and iii) can use the same method as ii). Denote $R = \left\{ a + b\frac{1+\sqrt{d}}{2} \,\middle|\, a, b \in \mathbb{Z} \right\}$. Take $r : \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}, a + b\sqrt{d} \to |a^2 - db^2|$ for $d \in \mathbb{Z}$, then we aim to find $q \in R$ such that $r(\frac{a+b\sqrt{2}}{c+d\sqrt{2}} - q) < 1$ for any $a+b\sqrt{d}, c+d\sqrt{d} \in R$. Note that for any $u+v\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ there exists $m+n\sqrt{-2} \in R$ such that $|u-m| < 1/4$ and $|v-n| < 1/4$, thus q exists.

9. Prove the invertible elements in $\mathbb{Z}[i]$ **where** $i = \sqrt{-1}$ **is** $\{\pm 1, \pm i\}$**.**

Proof. If $(a+bi)(c+di) = 1$, then $ac - bd = 1$ and $ad + bc = 0$. Since $a+bi$, $c+di$ are invertible and $\mathbb{Z}[i]$ is an ED with norm $a+bi \mapsto a^2+b^2$, we have $a^2+b^2 \leqslant 1$ and $c^2+d^2 \leqslant 1$. It deduces that all invertible elements in $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$. □

10. Let p be a prime, if $p \equiv 1(\bmod 4)$**, prove there exist** $a, b \in \mathbb{Z}$ **s.t.** $p = a^2 + b^2$**.**

Proof. If $p \equiv 1 \bmod 4$, then $G = (\mathbb{Z}/p\mathbb{Z})^\times$is a cyclic group of order $p-1$. Because $4 \mid p-1$ and G is cyclic, there is an element $\alpha \in G$ of order 4 . Thus, in $\mathbb{Z}[i]/(p)$, there are more than 2 solutions to the equation $x^2+1=0$, namely $\pm\alpha, \pm i \in \mathbb{Z}[i]/(p)$. Recall that the number of roots of a non-zero polynomial over commutative integral domain is at most its degree, so $\mathbb{Z}[i]/(p)$ is not an integral domain. Thus p is not prime and so is reducible in $\mathbb{Z}[i]$.

Assume that $p = (a+bi)(c+di)$ with $a+bi, c+di$ are non-units. Define $d : \mathbb{Z}[i] \to \mathbb{Z}, a+bi \mapsto a^2+b^2$, then we can verify $d(xy) = d(x)d(y)$ for any $x, y \in \mathbb{Z}[i]$. Hence we have $p^2 = d(p) = d(a+bi)d(c+di) = (a^2+b^2)(c^2+d^2)$. Since $a+bi$ is not invertible, $d(a+bi) \neq 1$ and $a^2+b^2 = p$. □