# 代数 1 H 班 作业 8

2022 年 11 月 10 日

**题 1.** 证明在 $R$-模 $M$ 中 $(-1)m = -m$.

**题 2.** 证明一个环的理想在环的乘法下做成环上的模。

**题 3** (Artin, Chapter 14, 1.2)**.** 假设 $V$ 上有阿贝尔群结构，将群结构的运算作为加法，如果 $V$ 上存在与这个加法相容的的 $\mathbb{Q}$-模结构，则这个 $\mathbb{Q}$-模结构被唯一确定。

**题 4.** 讨论和搞清楚期中没做出来的题目，不用交。

**题 5.** 记 $R$ 是 $\mathbb{Q}[\sqrt{d}]$ 的代数整数环。

1. 高斯证明了对以下的

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

$R$ 是 *UFD*。请挑选除了 $d = -1, -2, -3, -163$ 以外的某一个值证明高斯的结论。

2. (选做，不用交) 高斯还证明了对

$$-d = 5, 6, 10, 13, 15, 22, 35, 37, 51, 58, 91, 115, 123, 187, 235, 267, 403, 427,$$

$R$ 的类数 *(*通常记作 $h(d)$*)* 是 2. 请挑选除了 $d = -5$ 以外的一个例子证明高斯的结论. *(*高斯至少对较小的 $h(d) \leq 5$ 都列出来了 $d < 0$ 的列表，并猜测这些是对应类数的所有可能的 $d$. 最终问题的解决是上世纪七八十年代由 *Goldfeld-Gross-Zagier* 完成的，与 $L$ 函数有很大关系，最终对每一个类数 $h$ 可以转化成检验有限种情形的计算。*)*

**题 6** (PID 不是 ED)**.** 根据期中试题，我们知道欧几里德环 $R$ 的 *size* 函数 $s\colon R-\{0\}\to\mathbb{Z}_{\geq 0}$ 可以选做额外满足条件

$$\text{当非零元素 } a \mid b, \text{ 有 } s(a)\leq s(b). \tag{1}$$

请证明

1. 证明 $s(a)\geq s(1)$。
2. 当非零元素 $a$ 是 $b$ 的真因子的时候，有 $s(a)<s(b)$.
3. 证明 $s(a)=s(1)$ 当且仅当 $a$ 是乘法可逆元。
4. 假设 $R$ 不是域. 取 $a$ 是非单位元中使得 $s(a)$ 最小的元素，则 $a$ 不可约且 $R/(a)$ 的每个陪集的代表元都可选做 0 或者乘法可逆元。
5. 证明 $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ 不是 *ED*. （提示：用 $|R/(a)|=N(a)$ 来比较与 $|R^{\times}|$ 的的大小。）类似的可以证明 $-d=19,43,67,163$ 时对应的代数整数环不是 *ED*，其余几个是 *PID* 的虚二次域代数整数环是 *ED*.

**题 7** (Artin Chapter 13, 5.2)**.** *Let* $\delta=\sqrt{-3}$ *and* $R=\mathbb{Z}[\delta]$*. This is not the ring of integers in the imaginary quadratic number field* $\mathbb{Q}[\delta]$*. Let* $A$ *be the ideal* $(2,1+\delta)$*.*

1. *Prove that* $A$ *is a maximal ideal, and identify the quotient ring* $R/A$*.*
2. *Prove that* $\bar{A}A$ *is not a principal ideal, and that the Main Lemma is not true for this ring.*
3. *Prove that* $A$ *contains the principal ideal* $(2)$ *but that* $A$ *does not divide* $(2)$*.*

**题 8** (Artin Chapter 13, 6.7)**.** *Suppose that* $d<0\equiv 2$ *or* $3$ *modulo* $4$*, and that a prime* $p\neq 2$ *does not remain prime in* $R=\mathbb{Z}[\sqrt{d}]$*. Let* $a$ *be an integer such that* $a^2\equiv d$ *modulo* $p$ *(or we can say* $d$ *is a quadratic residue modulo* $p$*). Prove that* $(p,a+\delta)$ *is a lattice basis for a prime ideal that divides* $(p)$*.*

**题 9.**

1. $\mathbb{Z}[\sqrt{-5}]$ 中证明素理想 $I=(2,1+\sqrt{-5})$ 满足 $I=\bar{I}$。
2. 在 $\mathbb{Z}[i]$ 和 $\mathbb{Z}[\sqrt{-5}]$ 中，找到所有满足 $P=\bar{P}$ 的素理想 $P$。

*3.* 对一般的无平方因子的负整数 $d$，考虑 $R=\mathbb{Z}[a]$ 是 $\mathbb{Q}[\sqrt{d}]$ 的代数整数环。证明 $R$ 中的素理想 $P=\bar{P}$ 当且仅当

*(a)* $P=(p)$, $p$ 是素数，且在 $R$ 仍是素元.

*(b)* $P\bar{P}=(p)$，$p$ 是素数，且整除 $a$ 满足的二次首一多项式的判别式. *(称为 $p$ 在 $R$ 中分歧)*

**题 10** (丢番图问题中的应用)**.** 证明素数 $p\neq 2,5$ 时，$-5$ 在 $\mathbb{F}_p$ 中是某一个元素的平方（也称 $-5$ 是模 $p$ 的二次剩余）等价于存在整数 $a,b$, 使得 $p=a^2+5b^2$ 或者 $2p=a^2+5b^2$。（提示：利用前一题，以及 $\mathbb{Z}[\sqrt{-5}]$ 类群的结构.）二次剩余的理论能推出来此时 $p\equiv 1,3,7,9 \mod 20$.