THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 3030 Abstract Algebra 2023-24
Homework 10
Due Date: 4th December 2023

Compulsory Part

1. Prove that if p is an irreducible in a UFD, then p is a prime.

   Proof. Let p be an irreducible in a UFD R. Let $a, b \in R$. Suppose $p \mid ab$. Write $a = \pi_1 ... \pi_r$ and $b = \pi'_1 ... \pi'_s$, where π_i, π'_j are all irreducibles in R. Since $p \mid ab$, p is an associate of some π_i or π'_j. Then $p \mid a$ or $p \mid b$. That is, p is a prime. □

2. Let D be a UFD. Show that a non-constant divisor of a primitive polynomial in $D[x]$ is again a primitive polynomial.

   Proof. Recall that a polynomial is primitive if and only if 1 is a content of it. Suppose f is a primitive polynomial, and $f = g \cdot h$ where g is non-constant divisor. Then any content of f is a divisor of any content of g. But 1 is a content of f, so any content of g is a unit, i.e. 1 is a content of g. □

3. Let R be any ring. The **ascending chain condition (ACC) for ideals** holds in R if every strictly increasing sequence $N_1 \subset N_2 \subset N_3 \subset \cdots$ of ideals in R is of finite length. The **maximum condition (MC) for ideals** holds in R if every non-empty set S of ideals in R contains an ideal not properly contained in any other ideal of the set S. The **finite basis condition (FBC) for ideals** holds in R if for each ideal N in R, there is a finite set $B_N = \{b_1, \cdots, b_n\} \subseteq N$ such that N is the intersection of all ideals of R containing B_N. The B_N is a **finite generating set for** N.
   Show that for every ring R, the conditions ACC, MC, and FBC are equivalent.

   Proof. (ACC $\implies$ MC) Let R be a ring satisfying ACC but not MC. Then there is a nonempty set S of ideals of R without maximal element. Then for each ideal $N \in S$, there is an $N' \in S$ such that $N \subsetneq N'$.

   Let N_1 be an ideal in R. We can inductively define an ideal N_{i+1} of R with $N_{i+1} \supsetneq N_i$. This violates ACC. Therefore, ACC implies MC.

   (MC $\implies$ FBC) Let R be a ring satisfying MC. Let N be an ideal in R. Let S be the set of finitely generated ideals of R contained in N. Then S contains a maximal element N_1 by MC. Then $N_1 \subseteq N$ and N_1 is finitely generated. For any $a \in N$, $aR + N_1 \subseteq N$ is again finitely generated, and $N_1 \subseteq aR + N_1$. By the maximality of N_1, $N_1 = aR + N_1$. Then $a \in N_1$. Then $N = N_1$ is finitely generated.

   (FBC $\implies$ ACC) Let $N_1 \subsetneq N_2 \subsetneq \cdots$ be an infinite chain of ideals of R.

   Let $N = \bigcup_{i \geq 1} N_i$. Then N is an ideal of R. By FBC, there are $b_1, b_2, \ldots, b_n \in N$ such that $N = \langle b_1, b_2, \ldots, b_n \rangle$. For each i, b_i belongs to some N_{r_i}. Take r to be the maximum of the r_i's. Then, b_i belongs to N_r for all i.

   It follows that $N_r \subsetneq N_{r+1} \subseteq N = \langle b_1, b_2, \ldots, b_n \rangle \subseteq N_r$. Contradiction arises. Therefore, ACC holds. □

4. Prove or disprove the following statement: If ν is a Euclidean norm on Euclidean domain D, then $\{a \in D|\ \nu(a) > \nu(1)\} \cup \{0\}$ is an ideal of D.

   Answer. The statement is false, here is a counter-example.

   Let F be a field of characteristic $\neq 2$. Let $D = F[x]$, and $\nu(f) = \deg(f)$ is a Euclidean norm on D. Now both $1 + x$ and $1 - x$ have norm 1 which is greater than $0 = \nu(1)$. However, $(1 + x) + (1 - x) = 2$ has norm $0 \not> \nu(1)$.

   □

5. Show that every field is a Euclidean domain.

   Proof. Let F be a field. Define $\nu(x) = 1$ for all $x \in F^{\times}$. That $\nu(a) \leq \nu(ab)$ for $a, b \neq 0$ is clear. Now for $a, b \in F$ with $b \neq 0$, we have $a = (ab^{-1})b + 0$. Simply take $r = 0$. It follows that ν is a Euclidean norm on F. □

6. Let $\langle \alpha \rangle$ be a non-zero principal ideal in $\mathbb{Z}[i]$.

   (a) Show that $\mathbb{Z}[i]/\langle \alpha \rangle$ is a finite ring.

   (b) Show that if π is an irreducible of $\mathbb{Z}[i]$, then $\mathbb{Z}[i]/\langle \pi \rangle$ is a field.

   (c) Referring to part b, find the order and characteristic of each of the following fields.

      i. $\mathbb{Z}[i]/\langle 3 \rangle$

      ii. $\mathbb{Z}[i]/\langle 1 + i \rangle$

      iii. $\mathbb{Z}[i]/\langle 1 + 2i \rangle$

   Proof. (a) Recall that $\mathbb{Z}[i]$ is a Euclidean domain with a norm defined by $N(a + ib) = a^2 + b^2$.

   Note that $N(\alpha) \in \mathbb{Z}[i]$. Then for any $a, b \in \mathbb{Z}$, there exists some $0 \leq c, d \leq N(\alpha) - 1$ such that $a \equiv c \pmod{N(\alpha)}$ and $b \equiv d \pmod{N(\alpha)}$. Then $a + bi + \langle \alpha \rangle = c + di + \langle \alpha \rangle$. Since (c, d) has $|N(\alpha)|^2$ choices, $|\mathbb{Z}[i]/\langle \alpha \rangle| \leq |N(\alpha)|^2$.

   (b) Let π be an irreducible of $\mathbb{Z}[i]$. Then $\langle \pi \rangle$ is maximal among principle ideals other than $\mathbb{Z}[i]$.

   Since $\mathbb{Z}[i]$ is a Euclidean domain, it is a PID. Then $\langle \pi \rangle$ is maximal among all ideals other than $\mathbb{Z}[i]$. That is, $\langle \pi \rangle$ is a maximal ideal in $\mathbb{Z}[i]$. Then $\mathbb{Z}[i]/(\pi)$ is a field.

   (c) i. $\mathbb{Z}[i]/\langle 3 \rangle \simeq \mathbb{Z}[x]/(x^2 + 1, 3) \simeq \mathbb{F}_3[x]/(x^2 + 1)$. The order is 9 and the characteristic is 3.

      ii. $\mathbb{Z}[i]/\langle 1 + i \rangle \simeq \mathbb{Z}[x]/(x + 1, x^2 + 1) \simeq \mathbb{Z}[x]/(x + 1, 2) \simeq \mathbb{F}_2[x]/(x + 1) \simeq \mathbb{F}_2$. The order is 2 and the characteristic is 2.

      iii. $\mathbb{Z}[i]/\langle 1 + 2i \rangle \simeq \mathbb{Z}[x]/(1 + 2x, x^2 + 1) = \mathbb{Z}[x]/(5, x + 3) \simeq \mathbb{F}_5[x]/(x + 3) \simeq \mathbb{F}_5$. The order is 5 and the characteristic is 5.

   □

7. Let $n \in \mathbb{Z}^+$ be square free, that is , not divisible by the square of any prime integer. Let $\mathbb{Z}[\sqrt{-n}] = \{a + ib\sqrt{n} | a, b \in \mathbb{Z}\}$.

   (a) Show that the norm N, defined by $N(\alpha) = a^2 + nb^2$ for $\alpha = a + ib\sqrt{n}$, is a multiplicative norm on $\mathbb{Z}[\sqrt{-n}]$.

(b) Show that $N(\alpha) = 1$ for $\alpha \in \mathbb{Z}[\sqrt{-n}]$ if and only if α is a unit of $\mathbb{Z}[\sqrt{-n}]$.

(c) Show that every non-zero $\alpha \in \mathbb{Z}[\sqrt{-n}]$ that is not a unit has a factorization into irreducibles in $\mathbb{Z}[\sqrt{-n}]$.

Proof. (a) Note that $N(\alpha) = \alpha\overline{\alpha}$. Then for $\alpha, \beta \in \mathbb{Z}[\sqrt{-n}]$, $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta)$. It follows that N is multiplicative.

(b) Suppose α is a unit in $\mathbb{Z}[\sqrt{-n}]$. Then $\alpha\beta = 1$ for some $b \in \mathbb{Z}[\sqrt{-n}]$. Then $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$. Since the range of N is a subset of $\mathbb{Z}_{\geq 0}$, $N(\alpha) = 1$.

Conversely, suppose $\alpha \in \mathbb{Z}[\sqrt{-n}]$ has norm $N(\alpha) = 1$, then $\alpha\overline{\alpha} = 1$, and $\overline{\alpha} \in \mathbb{Z}[\sqrt{-n}]$. Therefore, α is a unit of $\mathbb{Z}[\sqrt{-n}]$.

(c) Suppose the statement is incorrect. Let $\alpha \in \mathbb{Z}[\sqrt{-n}]$ be a nonunit without such factorization such that any $\beta \in \mathbb{Z}[\sqrt{-n}] - \{0\}$ with $N(\beta) < N(\alpha)$ is either a unit or has a factorization into irreducibles in $\mathbb{Z}[\sqrt{-n}]$.

Then by (b), $N(\alpha) \geq 2$. Since α does not have factorization into irreducibles, α is not an irreducible itself. Then $\alpha = \beta\gamma$ for some nonunits $\beta, \gamma \in \mathbb{Z}[\sqrt{-n}]$. Then $N(\alpha) = N(\beta)N(\gamma)$, and $N(\beta), N(\gamma) \geq 2$. Then $N(\beta), N(\gamma) \leq N(\alpha)$, and so have factorization into irreducibles. Then α also has a factorization into irreducibles. Contradiction arises.

Therefore, every non-zero $\alpha \in \mathbb{Z}[\sqrt{-n}]$ that is not a unit has a factorization into irreducibles in $\mathbb{Z}[\sqrt{-n}]$.

□

Optional Part

1. Let R be any ring. The **descending chain condition (DCC) for ideals** holds in R if every strictly decreasing sequence $N_1 \supset N_2 \supset N_3 \supset \cdots$ of ideals in R is of finite length. The **minimum condition (mC) for ideals** holds in R if given any set S of ideals of R, there is an ideal of S that does not properly contain any other ideal in the set S.
   Show that for every ring, the conditions DCC and mC are equivalent.

   Proof. (DCC $\implies$ mC) Let S be a non-empty set of ideals of R. Suppose mC is false. Then for each $N \in S$, there is an $N' \in S$ such that $N' \subsetneq N$. Fix a member N_1 of S (possible since $S \neq \emptyset$). Then we define inductively an infinite sequence of ideals N_i such that $N_i \in S$ and $N_{i+1} \subsetneq N_i$ for all i. This contradicts the assumption of DCC.

   (mC $\implies$ DCC) Let $N_1 \supsetneq N_2 \supsetneq N_3 \supsetneq \cdots$ be an infinite strictly decreasing sequence of ideals of R. Let $S = \{N_i | i1\}$ be a non-empty set of ideals of R. Then mC implies that there is a member N_r of S which does not contain any other member of S. But this is impossible since $N_r \supsetneq N_{r+1}$. □

2. Give an example of a ring in which ACC holds but DCC does not hold.

   Answer. An example is given by $\mathbb{Z}$. That it satisfies ACC basically follows from the fact the every non-zero integer has a finite number of divisors. On the other hand, $\mathbb{Z}$ does not satisfies DCC because $2\mathbb{Z} \supsetneq 4\mathbb{Z} \supsetneq 8\mathbb{Z} \supsetneq \cdots \supsetneq 2^n\mathbb{Z} \supsetneq \cdots$.

3. Let ν be a Euclidean norm on a Euclidean domain D.

   a. Show that if $s \in \mathbb{Z}$ such that $s + \nu(1) > 0$, then $\eta : D^* \to \mathbb{Z}$ defined by $\eta(a) = \nu(a) + s$ for non-zero $a \in D$ is a Euclidean norm on D. As usual, D^* is the set of non-zero elements of D.

   b. Show that for $t \in \mathbb{Z}^+$, $\lambda : D^* \to \mathbb{Z}$ given by $\lambda(a) = t \cdot \nu(a)$ for non-zero $a \in D$ is a Euclidean norm on D.

   c. Show that there exists a Euclidean norm μ on D such that $\mu(1) = 1$ and $\mu(a) > 100$ for all non-zero non-units $a \in D$.

   Proof. **a,b.** Note first that if $\eta(1) = \nu(1) + s > 0$, then for any $a \in D^*$, $\eta(a) = \nu(a \cdot 1) + s \geq \nu(1) + s > 0$. The rest of the proof follows from the inequalities $\nu(a) \leq \nu(ab)$ and $\nu(r) < \nu(b)$ (from the division) about the norm ν because they imply immediately that $\eta(a) = \nu(a) + s \leq \nu(ab) + s = \eta(ab)$ (resp. $\lambda(a) = t \cdot \nu(a) \leq t \cdot \nu(ab) = \lambda(ab)$) and $\eta(r) = \nu(r) + s < \nu(b) + s = \eta(b)$ (resp. $\lambda(r) = t \cdot \nu(r) < t \cdot \nu(b) = \lambda(b)$).

   c. Take $\mu(a) = 100(\nu(a) - \nu(1)) + 1$ for $a \in D^*$. (Note that $a \in D^*$ is a unit if and only if $\nu(a) = \nu(1)$.) That μ is a Euclidean norm follows immediately from (a) and (b).

   □

4. Let D be a UFD. Show that all common multiples, in the obvious sense, of both a and b form an ideal of D.

Proof. Denote the set of all common multiples of a, b by $D(a, b)$,

- $x, y \in D(a, b) \Rightarrow x + y \in D(a, b)$:
  Let $x, y \in D(a, b)$. Then $a|x,\ b|x,\ a|y,\ b|y$. It follows that $a|(x + y),\ b|(x + y)$.
- $r \in R, x \in D(a, b) \Rightarrow rx \in D(a, b)$:
  Let $x \in D(a, b)$. Then $a|rx, b|rx$.

□

5. Let D be a UFD. An element c in D is a **least common multiple** (abbreviated lcm) of two elements a and b in D if $a|c, b|c$ and if c divides every element of D that is divisible by both a and b. Show that every two non-zero elements a and b of a Euclidean domain D have an lcm in D.

   Proof. Let D be a Euclidean domain and let a, b be two non-zero elements of D.

   Then D is a PID. Hence the ideal $\langle a\rangle \cap \langle b\rangle$ is principal. Let c be a generator of this ideal. Then $c \in \langle a\rangle$ and $c \in \langle b\rangle$, implying that $a|c$ and $b|c$. Suppose $c' \in D$ satisfies $a|c'$ and $b|c'$. Then c' belongs to $\langle a\rangle$ and $\langle b\rangle$, and hence to $\langle a\rangle \cap \langle b\rangle = \langle c\rangle$. It follows that $c|c'$. □