MATH 435 ASSIGNMENT 6

ARNOLD JIADONG YU

1. Chapter 18 Divisibility in Integral Domains

1.1. 30. Let p be a prime divisor of a postivie integer n. Prove that p is irreducible in Z_n if and only if p^2 divides n. (See Exercise 28)
proof: ($\Rightarrow$) Let p be a prime divisor of a positive integer n and p is irreducible in Z_n, but $p^2 \nmid n$. i.e. $n = kp$ for some $k \in Z_n$ and k, p are co-prime. i.e. $\gcd(\frac{n}{p}, p) = 1$. Therefore, there exists $s, t \in Z$ s.t.

$$s \cdot p + t \cdot \frac{n}{p} = 1 \Rightarrow sp^2 + tn = p$$

$$sp^2 \equiv p \pmod{n} \Rightarrow sp^2 - p \equiv 0 \pmod{n}$$
$$\Rightarrow p(sp-1) \equiv 0 \pmod{n} \Rightarrow sp - 1 \equiv 0 \pmod{n}$$
$$\Rightarrow sp \equiv 1 \pmod{n}$$

i.e. p is a unit, contradiction with p is irreducible. Hence $p^2|n$.
($\Leftarrow$) Suppose $p^2|n$ and p is not irreducible in Z_n. i.e. $p^2k = n$ for some $k \in Z_n$ and there exists non-unit elements $a, b \in Z_n$, s.t. $p \equiv ab \pmod{n}$.

$$p \equiv ab \pmod{n} \Rightarrow p = ab + xn \text{ (for some } x \in Z)$$

Since $p|n$, then $p|a$ or $p|b$ by Euclid's lemma. WLOG, assme $p|a$, and let $a = a^{'}p$ for some $a^{'} \in Z$. i.e.

$$p = ab + xn = a^{'}pb + x(p^2k) \Rightarrow 1 = a^{'}b + xpk$$

Therefore, $\gcd(b, pk) = 1$. i.e. $\gcd(b, p) = 1$ and $\gcd(b, k) = 1$. This implies $\gcd(b, p^2k) = 1$ which is the same as $\gcd(b, n) = 1$. This means b is a unit in Z_n. A contraction. Hence p is irreducible in Z_n. Therefore, p is irreducible in Z_n if and only if p^2 divides n.

1.2. 34. Show that $3x^2 + 4x + 3 \in Z_5[x]$ factors as $(3x+2)(x+4)$ and $(4x+1)(2x+3)$. Explain why this does not contradict the corollary of Theorem 18.3.
proof: The unit of $Z_5[x]$ is $1, 2, 3, 4$. By associate definition, $3x + 2$ is associate to $2x + 3$ since $3x + 2 = 4(2x + 3)$ in $Z_5[x]$. Also, $x + 4$ is associate to $4x + 1$ since $x + 4 = 4(4x + 1)$ in $Z_5[x]$. i.e. it doesn't contradict the corollary of Theorem 18.3 since $(3x + 2)(x + 4)$ and $(4x + 1)(2x + 3)$ are the same factorization.

1.3. 43. Prove that in a unique factorization domain, an element is irreducible if and only if it is prime.
proof: ($\Leftarrow$)Since in an integral domain, every prime is an irrducible. i.e. in a unique factorization domain, if an element is prime, then it is irrducible.
($\Rightarrow$) Let D be and unique factorization domain. Let $a \in D$ be an irreducible element and $a|bc$ for some $b, c \in D$.
case 1. If b, c are irreduible, then $ak = bc$ for some $k \in D$. This implies $a = b$ or $a = c$. Furthermore, $a|b$ or $a|c$.
case 2. If one of them is irreduible, WLOG assume b is irreduible, if $a = b$, we are done. Assume $a \neq b$, and $c = q_1^{n_1}...q_r^{n_r}$, where $q_1, ..., q_r$ are irreducible. i.e $a|bq_1^{n_1}...q_r^{n_r}$. Then $bq_1^{n_1}...q_r^{n_r} \equiv 0 \pmod a$, since $b \not\equiv 0 \pmod a$ implies $q_1^{n_1}...q_r^{n_r} \equiv 0 \pmod a$, i.e. $a = q_r$ for some r by induction. Hence, $a|c$. If c is irreducible and not equal to a, then $a|b$.
case 3) Assume b,c are not irreducible, and let $b = p_1^{m_1} \dots p_s^{m_s}$ and $c = q_1^{n_1}...q_r^{n_r}$ where $q_1, ..q_r, p_1, ..., p_s$ are all irreducible. Then

$$p_1^{m_1} \dots p_s^{m_s} q_1^{n_1}...q_r^{n_r} \equiv 0 \pmod a$$

$$\Rightarrow q_r \equiv 0 \pmod a \text{ for some r or } p_s \equiv 0 \pmod a \text{ for some s}$$

Since all q_r, p_s, a are irreducible, then $a = q_r$ for some r or $a = p_s$ for some s. i.e. $a|b$ or $a|c$.
Hence in a unique factorization domain, an element is irreducible if and only if it is prime.

1.4. 42*. Let $R = Z + Z + ...$ (the collection of all sequences of integers under componentwise addition and multiplication). Show that R has ideals $I_1, I_2, I_3, ...$ with the property that $I_1 \subset I_2 \subset I_3 ....$ (Thus R does not have the ascending chain condition.)
proof:

2. Resubmition of some homework questions

2.1. Homework 1. Page 71 #39. Let S be a subset of a group and let H be the intersection of all subgroups of G that contain S.
a. Prove that $< S > = H$.
b*. If S is nonempty, prove that $< S >= \{s_1^{n_1} s_2^{n_2} ... s_m^{n_m} | m \geq 1, s_i \in S, n_i \in Z\}$.(The s_i terms need not be distinct.)
proof: a. ($\Rightarrow$). WTS, $< S > \subseteq H$. Let H be the intersection of all subgroups of G that contain S, let K be an arbitrary subgroup of G contain S, then

$$H = \bigcap_{\forall K \leq G \text{ s.t. } S \subseteq K} K$$

Since K is a group itself and $S \subseteq K$, by definition $< S > \leq K$. Since H is the intersection of all those K and $< S >$ is subgroup of all those K, then $< S > \subseteq H$.
($\Leftarrow$) WTS: $H \subseteq < S >$. Let $h \in H$, then h is in the intersection of all those K contain S. That is $h \in K$ for $\forall K \leq G$ s.t. $S \subseteq K$. By definition, $< S >$ is the smallest subgroup of G contain S. That is $< S >$ is one of the K. Hence $h \in < S >$, this implies $H \subseteq < S >$. Therefore, $< S > = H$.

2.2. Homework 1 Page 157 #23. Suppose that H is a subgroup of S_4 and that H contains (12) and (234). Prove $H = S_4$.
proof: Let H be a subgroup of S_4, then $H \leq S_4$. Moreover H contains (12) and (234), $|(12)| = 2$ and $|(234)| = 3$. $(234)(12) = (1342)$ and $|(1342)| = 4$. That is $2, 3, 4$ divides $|H|$ and $|H|$ divides $|S|$ by Lagrange's Theorem. $|H| = 12$ or 24. Suppose $|H| = 12$, i.e. $H = A_4$ since $(1342) = (13)(14)(12)$ which is odd permutation i.e. $(1342) \in H$ but $(1342) \notin A_4$. A contradition. Hence $|H| = 24$ i.e. $H = S_{24}$.

2.3. Homework 4 Page 275 # 12. If A and B are ideals of a ring, show that the *product* of A and B, $AB = \{a_1b_1 + a_2b_2 + ... + a_nb_n | a_i \in A, b_i \in B, n$ a positive integer $\}$, is an ideal.
proof: Let R be a ring, and A, B are ideals of R. i.e. A, B are normal subgroup under addition, for any $a_i, c_i \in A, b_i, d_i \in B$, $a_i - c_i \in A, b_i - d_i \in B$ and any $r \in R$, $a_ir \in A, ra_i \in A$ and $b_ir \in B, rb_i \in B$.
(1) For $a_1b_1 + ... + a_nb_n, c_1d_1 + ... + c_md_m \in AB$.

$$(a_1b_1 + ... + a_nb_n) - (c_1d_1 + ... + c_md_m)$$

$$= a_1b_1 + ... + a_nb_n + (-c_1)d_1 + ... + (-c_m)d_m \in AB$$

Since , $a_i, -c_i \in A, b_i, d_i \in B$.
(2) For $a_1b_1 + ... + a_nb_n \in AB$ and $r \in R$,

$$(a_1b_1 + ... + a_nb_n)r = (a_1b_1)r + ... + (a_nb_n)r = a_1(b_1r) + ... + a_n(b_nr) \in AB$$

Since R is associative respect to multiplication and $a_i \in A, b_ir \in B$.

$$r(a_1b_1 + ... + a_nb_n) = r(a_1b_1) + ... + r(a_nb_n) = (ra_1)b_1 + ... + (ra_n)b_n \in AB$$

Since R is associative respect to multiplication and $ra_i \in A, b_i \in B$.
Hence AB is an ideal by Ideal Test.

2.4. Homework 5 Page 342 #37. An ideal A of a commutative ring R with unity is said to be *finitely generated* if there exist elements $a_1, a_2, ..., a_n$ of A such that $A = \langle a_1, a_2, ..., a_n \rangle$. An integral domain R is said to satisfy the *ascending chain condition* if every strictly increasing chain of ideals $I_1 \subset I_2 \subset ...$ must be finite in length. Show that an integral domain R satisfies the ascending chain condition if and only if every ideal of R is finitely generated.
proof: ($\Rightarrow$) Prove by contrapositive. Assume there exsits an ideal I of R is not finitely generated. Let $a_0 \in I$. Then $\langle a_0 \rangle \subsetneq I$ since i is not finitely generated. There exists $a_1 \in I \backslash \langle a_0 \rangle$ s.t. $\langle a_0 \rangle \subsetneq \langle a_0, a_1 \rangle$. Continue doing this and find out this strictly increasing chain of ideals is infinite in length. Hence if an integral domain R satisfies the ascending chain condition then every ideal of R is finitely generated.
($\Leftarrow$) Suppose every ideal of R is finitely generated, and there exists a strictly increasing chain of ideals $I_1 \subset I_2 \subset I_3 ...$, WTS it is finite. Let $I = \bigcup I_i$, then I is an ideal. Moreover $I = \langle a_1, ..., a_n \rangle$ where n is finite. Then $a_i \in I_{m_i}$ where m_i is the index of a ideal in the chain of ideals. Let $s = \max(m_1, ..., m_n)$. Then $a_j \in I_s$ for all $a_j \in \{a_1, \ldots a_n\}$, i.e. $I_s = I$. So, the ascending chain condition satisfied.
Hence an integral domain R satisfies the ascending chain condition if and only if every ideal of R is finitely generated.