HOMEWORK 2

Due date: Tuesday of Week 3

Ex: 4.3, 5.1, 5.3, 5.5, 5.6, 5.7, 6.1, 6.2, 6.8, 7.1, 7.2, 7.5, 8.1, 8.2, 8.3, 8.4. Pages 355-357 of Artin's book.

Here are some terminologies. Let R be a ring. Two ideals I, J of R are called coprime (or relatively prime) if $I + J = R$. (Recall that two positive integers m, n are called coprime if their gcd is 1, which is equivalent to $(m) + (n) = \mathbb{Z}$. Thus the new definition agrees with the old one in the case when $R = \mathbb{Z}$).

Problem 1 (Chinese Remainder Theorem (Exercise 6.8))**.** *Let I, J are two coprime ideals of R. Show that*

$$R/(I \cap J) \cong (R/I) \times (R/J).$$

This is essentially Exercise 6.8. For example, if m, n are two relatively prime integers, we have $\mathbb{Z}/(mn) \cong \mathbb{Z}/(m) \times \mathbb{Z}/(n)$ as a ring. We learned this last semester.

Problem 2.

1. *Let R_1, R_2 be two rings and $R = R_1 \times R_2$. Show that there is a bijection $R^\times \cong R_1^\times \times R_2^\times$.*
2. *Let p be a prime integer, show that $|(\mathbb{Z}/p^k\mathbb{Z})^\times| = p^k - p^{k-1}$.*
3. *Let n be a positive integer and let $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. Compute $\varphi(n)$, which can be interpreted as the number of integers in $\{0, 1, 2, \ldots, n-1\}$ which is coprime to n.*
4. *Let a, n be two positive integers such that a is coprime to n. Show that $a^{\varphi(n)} \equiv 1 \bmod n$. As a special case, if p is a prime number and if $p \nmid a$, then $a^{p-1} \equiv 1 \bmod p$.*

Hint for (2): Use Chinese remainder theorem to decompose $\mathbb{Z}/n\mathbb{Z}$ into product of rings. The function $\varphi(n)$ is called the Euler function. The congruence relation $a^{p-1} \equiv 1 \bmod p$ is called Fermat's little theorem. The congruence $a^{\varphi(n)} \equiv 1 \bmod n$ is a generalized of Fermat's little theorem given by Euler.

Problem 3. *Let I be an ideal of a ring R. Show that I is prime if and only if R/I is an integral domain.*

Problem 4. *Let R be a ring and let $x \in R$ be a nilpotent element. Show that $1 + x$ is a unit. Moreover, if $u \in R^\times$, show that $u + x$ is also a unit.*

Problem 5. *Let R be a ring and let $f = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. Show that*

1. *$f \in R[x]^\times$ iff $a_0 \in R^\times$ and $a_1, \ldots, a_n$ are nilpotent.*
2. *f is nilpotent iff $a_0, a_1, \ldots, a_n$ are nilpotent.*
3. *f is a zero divisor (which means there exists a nonzero $g \in R[x]$ such that $fg = 0$) iff there exists $a \neq 0$ in R such that $af = 0$.*

This is Exercise 2 from the book Atiyah-Macdonald, *Introduction to commutative algebra*, Chapter I. (Hint: For (1), if $g = b_0 + b_1x + \cdots + b_mx^m$ is the inverse of f, prove by induction on r that $a_n^{r+1}b_{m-r} = 0$. Hence show that a_n is nilpotent and then use the assertion of the last problem.) (For (3), choose a polynomial $g = b_0 + b_1x + \cdots + b_mx^m$ of least degree m such that $fg = 0$. Then $a_nb_m = 0$. Note that $\deg(a_ng) < \deg(g)$ and $a_ngf = 0$. The minimality of the degree of g shows that $a_ng = 0$. Then show $a_{n-r}g = 0$ by induction on r).

Let R be a ring and $S \subset R$ be a multiplicative set (which means $0 \notin S$ and S is closed under multiplication: $\forall a, b \in S$, we have $ab \in S$). Denote by $S^{-1}R$ the set of S-fractions, see Exercise 7.5 if R is an integral domain. More precisely, we define an equivalence relation $\sim$ on the set $R \times S$ by

$$(r, s) \sim (r', s') \iff u(r's - rs') = 0 \text{ for some } u \in S.$$

Notice that if R is integral domain, the above equivalence relation is the same as $r's = rs'$, which is given in Exercise 7.5. Similar to Exercise 7.5, $\sim$ is an equivalence relation. Check this! For $a \in R, s \in S$, we denote by a/s the equivalence class of (a, s). Let $S^{-1}R$ be the set of equivalence classes, which has a natural ring structure defined as usual

$$a/s + b/t = (at + bs)/(st),$$
$$(a/s)(b/t) = (ab)/(st).$$

Problem 6. *Let $\mathfrak{p}$ be a prime ideal of a ring R. Let $S = R - \mathfrak{p} = \{x \in R : x \notin \mathfrak{p}\}$. Show that S is a multiplicative set. The resulted ring $S^{-1}R$ will be denoted by $R_{\mathfrak{p}}$.*

A ring R is called a local ring if it has exactly one maximal ideal $\mathfrak{m}$. The field $R/\mathfrak{m}$ is called the residue field of R.

Problem 7.
(1) *Let R be a ring and I be a maximal ideal of R. Suppose that for any $x \in I$, $1 + x$ is a unit in R. Show that R is a local ring and thus I is the unique maximal ideal of R.*
(2) *Let R be a ring and $\mathfrak{p}$ be a prime ideal of R. Show that $R_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. What is the relation between $R/\mathfrak{p}$ and $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$?*

The local ring $R_{\mathfrak{p}}$ is called the localization of R at $\mathfrak{p}$.

Problem 8. *Let p be a prime integer. Describe $\mathbb{Z}_{(p)}$, the localization of $\mathbb{Z}$ at the prime (p). Let n be any nonzero integer. Describe the ideal $n\mathbb{Z}_{(p)}$ (the ideal of $\mathbb{Z}_{(p)}$ generated by n).*

Problem 9. *Let R be a ring and let $\mathfrak{m}$ be a maximal ideal of R. Show that $\mathfrak{m}$ is prime.*

Problem 10. *Show that any vector space V over a field F has a basis using Zorn's lemma.*

See the appendix of Artin's book, Proposition A.3.3, page 518.

Problem 11. *Let R be a ring and I be an ideal of R such that $I \neq R$. Show that there exists a maximal ideal $\mathfrak{m} \subset R$ such that $I \subset \mathfrak{m} \subset R$.*

This is covered in class. Please repeat the proof here.

Problem 12. *Let R be a ring. Show that the nilradical of R is the intersection of all prime ideals of R.*

Hint: from last HW, we know that the nilradical is contained in the intersection of all prime ideals. To show the converse, by contradiction, suppose that a is in the intersection of all prime ideals, but not nilpotent. Consider the set of all ideals I such that $a^n \notin I$ for any $n > 0$. Using Zorn's lemma to show that there is a maximal ideal in S and show this maximal element is a prime ideal.