MATH 504
EXERCISES 5

A. ZEYTİN

Unless otherwise stated R is a ring.

(1) Let X be a subset of R. Recall that we defined the ideal generated by X as the smallest ideal containing X, and denote it by (X).
  - ▶ Show that $[X] = \{r_1 x_1 + \ldots + r_n x_n : r_i \in R,\ x_i \in X \text{ for all } i = \{1, \ldots, n\}, i \in \mathbf{N}\}$ is an ideal of R.
  - ▶ Show that $(X) = [X]$.

(2) Let R be a commutative ring with 1 and I be an ideal of R. We define the radical of I as :

$$\sqrt{I} := \{\alpha \in R \colon \alpha^n \in I \text{ for some } n \in \mathbf{N}\}.$$

  - ▶ Show that $\sqrt{I}$ is an ideal of R containing I.
  - ▶ Let $\mathfrak{p}$ be a prime ideal of R. Show that $\sqrt{\mathfrak{p}} = \mathfrak{p}$. (Such an ideal is called a *radical ideal*.)
  - ▶ For $I = (16) \leq \mathbf{Z}$ compute $\sqrt{I}$.
  - ▶ For $I = (6) \leq \mathbf{Z}$ compute $\sqrt{I}$.
  - ▶ For $I = (16) \leq \mathbf{Z}/144\mathbf{Z}$ compute $\sqrt{I}$.
  - ▶ Is $I = \{0\} \leq \mathbf{Z}/n\mathbf{Z}$ a radical ideal when $n = 6, 9, 12, 15$.
  - ▶ Show more generally that $\{0\} \leq \mathbf{Z}/n\mathbf{Z}$ is a radical ideal if and only if n is a square-free integer.
  - ▶ Use previous exercise to show that $(n) \leq \mathbf{Z}$ is a radical ideal if and only if the integer n is square-free.
  - ▶ Show that $\sqrt{\sqrt{I}} = \sqrt{I}$ for any ideal I of R.
  - ▶ Show that $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

(3) Let S be a non-empty multiplicative subset of the commutative ring with 1 R and let $s_o \in S$
  - ▶ Show that the map $\iota \colon R \to S^{-1}R$ defined by sending $\alpha \in R$ to the pair $\iota(\alpha) = (\alpha s_o, s_o)$ is a ring homomorphism.
  - ▶ Show that if $\alpha \in S$ then $\iota(\alpha)$ is a unit in $S^{-1}R$.
  - ▶ Show that if $\iota(\alpha) = (0, s_o)$, then αs must be 0 for some $s \in S$ (hence α is a zero-divisor)

(4) Let $\varphi \colon R \to R'$ be a ring homomorphism between two rings R and R' and let S be a multiplicative subset of R. Show that if $\varphi(s)$ is a unit in R' for all $s \in S$, then φ induces a unique homomorphism $\widetilde{\varphi} \colon S^{-1}R \to R'$. Why do we need $\varphi(s) \in R'$ to be a unit?

(5) Let S be a multiplicative subset of the commutative ring with 1 R. Show that there is a one to one correspondence between :

$$\{\mathfrak{p} \leq R \colon \mathfrak{p} \cap S = \emptyset\} \text{ and } \{\mathfrak{q} \leq S^{-1}R \colon \mathfrak{q} \text{ is a prime ideal}\}.$$

Deduce that if $\mathfrak{p}$ is a prime ideal of R then there is a one-to-one correspondence between the prime ideals of R contained in $\mathfrak{p}$ and the prime ideals of $A_{(\mathfrak{p})} = S^{-1}R$; where $S = R \setminus \mathfrak{p}$.

(6) Let $R = \mathbf{Z}[\sqrt{-1}]$, i.e. the ring of Gaussian integers and for any element $\alpha = a + b\sqrt{-1} \in R$; where $a, b \in \mathbf{Z}$, define the norm of α as $N(\alpha) = a^2 + b^2$.
  - ▶ Show that N is a norm on R.
  - ▶ Show that $N(\alpha) = 0$ if and only if $\alpha = 0$.
  - ▶ Show that form any $\alpha, \beta \in R$ $N(\alpha\beta) = N(\alpha)N(\beta)$.
  - ▶ Give a criterion for norms of units in R.
  - ▶ Show that R is an integral domain.
  - ▶ Show that R is an integral domain with the above norm. Hint: Given any non-zero $\alpha, \beta \in R$, write $\alpha/\beta = a + b\sqrt{-1}$ with $r, s \in \mathbf{Q}$. Choose q_1, q_2 to be the integers closest to a and b, respectively. Set $q = q_1 + q_2\sqrt{-1}$ and $r = a - b\,q$.
  - ▶ Using the fact that R is an Euclidean domain find q and r in R so that $7 + 2\sqrt{-1} = (3 - 4\sqrt{-1})q + r$.

- Using the fact that R is an Euclidean domain find the greatest common divisor of $8+6\sqrt{-1}$ and $5-15\sqrt{-1}$ in R.
- Let α be any non-zero element of R. Show that the ring $R/(\alpha)$ is a finite ring. Hint: Use again the fact that R is a Euclidean domain.
- Determine the following rings : $R/(3)$, $R/(1+\sqrt{-1})$ and $R/(1+2\sqrt{-1})$.

(7) Decide whether being associates ($\alpha \sim \beta :\Leftrightarrow$ there is some u unit in R so that $\alpha = u\beta$) is an equivalence relation.

(8) Let $R = \mathbf{Z}/2\mathbf{Z}[x]$ and set $N(f(x)) := \deg(f(x))$.
- Show that N defines a norm on R.
- Determine all the units in R.
- Show that $p(x) = x^2 + x + 1$ is irreducible in R. Deduce that $k = R/(p)$ is a field.
- Write out the addition and multiplication tables of k.

(9) Let R be a UFD and a, b and $a_0, a_1, \dots, a_n$ be non-zero elements of R.
- Define a greatest common divisor for a and b.
- Define a greatest common divisor for more than 2 elements, say $a_0, a_1, \dots, a_n$. Denote it by $\gcd(a_0, \dots, a_n)$. Give an explicit example to see that $\gcd(a_0, \dots, a_n)$ may not be unique.
- A non-constant polynomial $f(x) = a_0 + a_1 t + \dots + a_n x^n \in R[x]$ is called *primitive* if 1 is a greatest common divisor of $a_0, \dots, a_n$.
- Decide whether $4x^2 + 7x - 2$ is primitive in $\mathbf{Z}[x]$.
- Decide whether $4x^3 + 6x - 10$ is primitive in $\mathbf{Z}[x]$.
- Show that for any non-constant polynomial $f(x) \in R[x]$ there is some elements $c \in R$ so that $f(x) = c\, g(x)$ where $g(x) \in R[x]$ is primitive. Show that c is uniquely determined up to multiplication by units. Such a c is called the content of f.
- Find the content of $4x^3 + 6x - 10 \in \mathbf{Z}[x]$.
- Show that if $f(x), g(x) \in R[x]$ are primitive then their product is also primitive. Use induction to deduce that the product of finitely many primitive polynomials is again primitive.
- Show that if $f(x)$ is a non-constant primitive element of $R[x]$ and gx is a divisor of $f(x)$, then $g(x)$ is also primitive.