Due: Friday, Oct 19, 2018

Math 371 / Problem Set 4 (2 pages)

- **Study/read**:
  - Ch. 7, 8, 9 of *Abstract Algebra* by Dummit–Foote.
  - Ch. IV, 18-23, Ch. V, 26-27 of *Abstract Algebra* by Fraleigh.

(!) Make sure that you understand perfectly the definitions, examples, theorems, etc.

- **Solve the problems below:**

1) Let R be a finite commutative ring, $1 \neq 0$. Show that every element of R is either invertible or a zero divisor.

2) Answer/prove/disprove the following:

a) Let $R := \mathbb{Z}/60\mathbb{Z}$ and $D \subset R$ be the multiplicative system D generated by $\overline{3}, \overline{4}$. What is $D^{-1}R$?

b) Every ring of fractions of $\mathbb{Z}/m\mathbb{Z}$ is isomorphic to $\mathbb{Z}/m_1\mathbb{Z}$ for some m_1.

c) The same question for an abstract ring R in which every element is either a zero divisor or invertible.

3) Let $R = \times_{i \in I} R_i$ be the product of a family of rings R_i with $0 \neq 1$. If I is finite, prove/disprove the following questions from the class:

a) $\mathfrak{a} \subset R$ is a left/right/two sided ideal iff $\mathfrak{a} = \times_{i \in I} \mathfrak{a}_i$ with $\mathfrak{a}_i \subset R_i$ left/right/two sided ideals.

- For $\mathfrak{a} \subset R$ a two sided ideal, how does the factor ring $R/\mathfrak{a}$ relate to the factor rings $R/\mathfrak{a}_i$, $i \in I$?

b) R is commutative iff R_i is commutative for all $i \in I$. Further let R_i be commutative. Then one has:

- $\mathfrak{a} \subset R$ is a prime ideal iff there exists $i_0 \in I$ s.t. $\mathfrak{a} = \times_{i \in I} \mathfrak{a}_i$ with $\mathfrak{a}_{i_0} \subset R_{i_0}$ prime ideal and $\mathfrak{a}_i = R_i$ for $i \neq i_0$.
- What is the factor ring $R/\mathfrak{a}$ for $\mathfrak{a}$ a prime ideal?

• The same questions concerning maximal ideals $\mathfrak{m} \subset R$.

$(*)$ The same questions for I not necessarily finite.

Recall that a map $N : R \to \mathbb{N}$ on a ring R is called multiplicative, if

$$N(ab) = N(a)N(b) \text{ for all } a, b \in R.$$

4) Prove that the sets R below are subrings of the real or complex numbers, and that the given maps $N : R \to \mathbb{N}$ are Euclidean multiplicative norms:

a) $R = \mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subset \mathbb{R}$,
$N : R \to \mathbb{N}$ by $N(a + b\sqrt{2}) := |a^2 - 2b^2|$.
- Are the principal ideals $2R, 3R, 5R, 7R, 17R$ prime ideals?

b) $R = \mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$, where i is the 4th root of unity,
$N : R \to \mathbb{N}$ by $N(a + bi) := a^2 + b^2$.
- Are the principal ideals $2R, 3R, 5R, 7R, 17R$ prime ideals?

c) $R = \mathbb{Z}[\,\zeta_3] := \{a + b\,\zeta_3 \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$, where $\zeta_3^3 = 1$, $\zeta \neq 1$,
$N : R \to \mathbb{N}$ by $N(a + b\zeta_3) := |a + b\zeta_3|^2$ is square of the absolute value of the complex number $a + b\zeta_3$.
- Are the principal ideals $2R, 3R, 5R, 7R, 17R$ prime ideals?

5)* Are there Euclidean norms on $R = \mathbb{Z}[\sqrt{-5}] := \{a+b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$, respectively $R = \mathbb{Z}[\sqrt{5}] := \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{R}$?

6) Prove/disprove the following assertions:

a) The polynomial ring $\mathbb{Z}[t]$ does not carry any Euclidean norm.

b) Let R be a domain. Then the polynomial ring $R[t]$ allows an Euclidean norm iff R is a field.

[**Hints**: To a): It suffices to show that $\mathbb{Z}[t]$ is not a PID (WHY), etc. To b): Show that if $r \in R$ is not invertible, then $(r, t) := \{rx + ty \mid x, y \in R[t]\}$ is a non-principal ideal (WHY), etc.

Reading: Study Section 7.6 *The Chinese Remainder Theorem* of Ch. 7 from *Abstract Algebra* by Dummit–Foote.

7) Answer/Prove the following:

a) The map $\mathbb{Z}/2020\,\mathbb{Z} \to \mathbb{Z}/101\,\mathbb{Z} \times \mathbb{Z}/4\,\mathbb{Z}$, $a + 2020\,\mathbb{Z} \mapsto (a + 101\,\mathbb{Z},\ a + 4\,\mathbb{Z})$ is well defined and surjective.

b) Find all $x \in \mathbb{Z}$ such that $x \equiv 1 (\bmod 101)$ and $x \equiv 2 (\bmod 5)$.

c) The map $\phi : \mathbb{Q}[t] \to \mathbb{Q}^n$, $p(t) \mapsto \big(p(1), \ldots, p(n)\big)$ is a surjective ring homomorphism. What is $\mathrm{Ker}(\phi)$?
- Does the same hold if we replace $\mathbb{Q}$ by $\mathbb{Z}$?

d) What is the image of $\mathbb{Q}[t] \to \mathbb{R}^n$ defined by $p(t) \mapsto \big(p(\sqrt{a_1}), \ldots, p(\sqrt{a_n})\big)$, where $a_1, \ldots, a_n \in \mathbb{N}$ are relatively prime?