Abstract Algebra in Theoretical Computer Science

Assignment 2

Lecturer: Gil Cohen

Problem 1 - Prime ideals

Let R be a commutative ring. Recall that a *prime ideal* P in R is an ideal $P \neq R$ such that for every $r, s \in R$, if $rs \in P$ then at least one of r, s is also in P. Recall further that, informally speaking, prime ideals abstract the notion of primality that is familiar to us from the integers. Indeed, a number $p \in \mathbb{Z}$ is prime whenever $p|ab$ implies that $p|a$ or $p|b$ (or both). Recall that an ideal I is maximal if and only if R/I is a field. That is, the maximality of an ideal is completely characterized by the respective quotient. A similar phenomena holds for prime ideals.

1. Let I be an ideal in a commutative ring R. Prove that I is prime if and only if R/I is an integral domain. Conclude that any maximal ideal is prime.

In $\mathbb{Z}$ every prime ideal is maximal but there are rings in which a prime ideal must not be maximal. Nevertheless, if the ring is a PID every prime ideal is maximal. You are asked to prove these two facts in the following two items.

2. Give an example of a prime ideal that is not maximal.

3. Prove that in a PID every prime ideal is maximal.

Problem 2 - The radical of an ideal

For an ideal I in a commutative ring R we define the *radical of* I by

$$\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{N}\}.$$

Informally, the radical attempts to abstract the idea of "striping off" multiplicities as you will see in the next two items.

1. Let k be a field and $R = k[x]$. Prove that $\sqrt{\langle x^4 \rangle} = \langle x \rangle$.

2. What is $\sqrt{12\mathbb{Z}}$ in the ring $\mathbb{Z}$?

3. Prove that $\sqrt{I}$ is an ideal.

4. Prove that $\sqrt{P} = P$ for every prime ideal P.

Let R be a commutative ring. We define $\mathrm{Spec}(R)$ to be the set of all prime ideals in R.

5. Prove that
$$\sqrt{I} = \bigcap_{\substack{P \in \mathrm{Spec}(R) \\ I \subseteq P}} P.$$
Observe that this implies the previous item, but try to prove the previous item without using this one. Showing additive closeness is a bit tricky.

Problem 3 - Finite integral domains are fields

Recall that every field is a PID (simply because it has only two ideals: $\langle 0 \rangle, \langle 1 \rangle$) and hence an integral domain. Prove that every *finite* integral domain is a field.

Problem 4 - Fields and integral domains

Let R be a commutative ring. Consider the map $\phi\colon R[x] \to R$ that is given by $\phi(f(x)) = f(0)$.

1. Prove that ϕ is a ring homomorphism. This homomorphism is nothing but an algebraic way to express evaluation of a polynomial at 0.
2. Prove that $R[x]/\langle x \rangle \simeq R$.
3. Prove that if $R[x]$ is a PID then R is a field.

Problem 5 - Units

Let R be a commutative ring. An element $r \in R$ is a *unit* if there exists $s \in R$ such that $rs = 1$.

1. Prove that the units in a commutative ring form a group under multiplication.
2. Find the group of units in $\mathbb{Z}[i]$.
3. Prove that there are infinitely many units in $\mathbb{Z}[\sqrt{2}]$.

Problem 6 - A field with 9 elements

In class we showed that for every prime number p there exists a field of size p. In this exercise, you are asked to construct a field that consists of 9 elements. To this end, consider the ideal $\langle 3 \rangle$ in $\mathbb{Z}[i]$.