Problems 3

1 Prime ideals

Let R be a ring and $P \subset R$ an ideal. The ideal P is called *prime* if $ab \in P \Rightarrow a \in P$ or $b \in P$.

1. Let R be a ring and let $a \in R$. Show that the ideal (a) is prime if and only if a is a prime element of R.
2. Let R be a ring and $P \subset R$ a proper ideal. Show that the following conditions are equivalent.
   (a) P is a prime ideal ;
   (b) R/P is an integral domain ;
   (c) Let A, B ideals such that $AB \subset P$. Then $A \subset P$ or $B \subset P$.
3. Let R be a finite integral domain. Show that R is a field.

2 Algebraic numbers

Which of the following complex numbers are algebraic ? Which are algebraic integers ?

1. $355/113$;
2. $e^{2\pi i/23}$;
3. $e^{\pi i/23}$;
4. $\sqrt{17} + \sqrt{19}$;
5. $\dfrac{1+\sqrt{17}}{2\sqrt{-19}}$;
6. $\sqrt{1+\sqrt{2}} + \sqrt{1-\sqrt{2}}$.

3 Exercise on Gaussian integers from last recitation

Our goal is to show that a prime $p \in \mathbb{Z}$ is a sum of two squares if and only if $p = 2$ or $p \equiv 1[4]$.

1. We denote $S = \{p \in \mathbb{Z} \text{ prime}, \exists\ a, b \in \mathbb{Z},\ p = a^2 + b^2\}$. Show that $p \in S \iff p$ is reducible in $\mathbb{Z}[i]$.
2. Show that $\mathbb{Z}[i]/(p)$ is an integral domain if and only if -1 is not a square in $\mathbb{F}_p$.
3. Deduce the result in the case where $p = 2$.
4. Case $p > 2$. Show that $x \in \mathbb{F}_p$ is a square if and only if $x^{\frac{p-1}{2}} = 1$. Deduce the result.