MTH 411: Final exam
Fall 2015

Duration: 120 min
The problems are independent

Exercise 1:
What is the degree of $\mathbb{Q}(\sqrt[3]{2}, \sqrt[5]{3})$ over $\mathbb{Q}$?

Exercise 2:
Let p be a prime number and let G be the subgroup of S_p generated by $(1234\dots p)$.
Show that G is a Sylow p-subgroup of S_p.

Exercise 3:
Show that $\mathbb{Q}(\sqrt[5]{2}, e^{\frac{2i\pi}{5}})$ is a splitting field of $X^5 - 2$.

Problem 1:
Let $\omega_n = e^{\frac{2i\pi}{n}}$
$P_n(X) = X^n - 1 \in \mathbb{Q}[x]$
$\mathbb{U}_n = \{\omega_n^k,\ k = 0 \dots n\}$
1) Show that $\mathbb{U}_n$ is the set of all roots of P_n.
2) Show that $\mathbb{Q}(\omega_n)$ is the splitting field of P_n over $\mathbb{Q}$.
3) Show that $\mathbb{U}_n$ is a group under multiplication, isomorphic to $\mathbb{Z}_n$ and that ω_n^k is a generator of $\mathbb{U}_n$ if and only if $gcd(k, n) = 1$
4) Show that if $\psi : \mathbb{Q}(\omega_n) \longrightarrow \mathbb{Q}(\omega_n)$ is an isomorphism of fields then $\varphi(\omega_n)$ is a generator of $\mathbb{U}_n$
5) Deduce from 4) that the degree $[\mathbb{Q}(\omega_n) : \mathbb{Q}]$ is at most $\varphi(n)$ the number of generators of $\mathbb{U}_n$.
(Hint: Show that the roots of the minimal polynomial of ω_n are all generators of $\mathbb{U}_n$.)

Problem 2:
Let

$$A = \{a^2 + b^2,\ \ a, b \in \mathbb{Z}\} = \{N(z),\ z \in \mathbb{Z}[i]\}$$

where $N : \mathbb{Z}[i] \to \mathbb{Z}$ is the norm function $N(a + bi) = a^2 + b^2$.

1) Let $p \in \mathbb{Z}$ be prime.
Compute $N(p)$ and show that p is irreducible in $\mathbb{Z}[i]$ if and only if $p \notin A$

From now on we assume that p is prime and that $p = 1 + 4k$ with $k \in \mathbb{Z}$.
2)Why is $(\mathbb{Z}_p^*, \times)$ a cyclic group? What is its order?

Let y be a generator of $(\mathbb{Z}_p^*, \times)$.
3) Show that y^k is a solution of the equation $z^2 + 1 = 0$ $(mod\ p)$.
4) Let m such that $m^2 + 1 = 0$ $(mod\ p)$.
We denote by (p) the ideal in $\mathbb{Z}[i]$ generated by p.
Using that $(m + i)(m - i) \in (p)$, show that (p) is not a prime ideal
5) Conclude that $p \in A$.