MTH 411: Final exam
Fall 2016

Duration: 120 min
The problems are independent

Exercise 1:
What is the degree of $\mathbb{Q}(\sqrt{2}, i\sqrt{2}, \sqrt[5]{7})$ over $\mathbb{Q}$?

We know that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, also $[\mathbb{Q}(\sqrt{2}, i\sqrt{2}) : \mathbb{Q}(\sqrt{2})] \leq 2$ because $i\sqrt{2}$ is a root of $X^2 + 2$. This degree is actually 2 as $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ and $\mathbb{Q}(\sqrt{2}, i\sqrt{2}) \not\subseteq \mathbb{R}$. So $[\mathbb{Q}(\sqrt{2}, i\sqrt{2}) : \mathbb{Q}] = 4$.

On the other hand, $\mathbb{Q}(\sqrt{2}, i\sqrt{2}, \sqrt[5]{7})$ contains $\mathbb{Q}(\sqrt[5]{7})$ which has degree 5 over $\mathbb{Q}$ by Eisenstein criterion for $X^5 - 7$. So the degree $[\mathbb{Q}(\sqrt{2}, i\sqrt{2}, \sqrt[5]{7}) : \mathbb{Q}]$ is divisible by 4 and 5 so it is divisible by 20. But $[\mathbb{Q}(\sqrt{2}, i\sqrt{2}, \sqrt[5]{7}) : \mathbb{Q}((\sqrt{2}, i\sqrt{2})] \leq 5$ so this degree is exactly 20.

Exercise 2:
Let G be a group of order 325. Show that G is abelian.

By the third Sylow theorem, let us compute the number of 5 and 13-Sylow of G.

$n_5 \equiv 1 (\text{mod } 5)$ and $n_5 | 13$ so $n_5 = 1$.

$n_13 \equiv 1 (\text{mod } 13)$ and $n_{13} | 25$, so $n_{13} = 1$.

Then, both the 5-Sylow S_5 and the 13-Sylow S_13 of G are unique, thus normal by the second Sylow theorem. Their intersection is the trivial subgroup, so $G \simeq S_5 \times S_13$. But S_13, of cardinal 13, is isomorphic to $\mathbb{Z}_13$, and S_5, of cardinal 25, is isomorphic to $\mathbb{Z}_{25}$ or to $\mathbb{Z}_5 \times \mathbb{Z}_5$.

Thus G is abelian.

Exercise 3:
Compute a^2 (mod 13) for $a \in \mathbb{Z}_{13}$, then show that 2 is irreducible in $\mathbb{Z}[\sqrt{13}]$.

For $a = 0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6$, $a^2 = 0, 1, 4, -4, 3, -1, -3$ modulo 13. So neither 2 nor -2 is a square mod 13.

If $2 = xy$ with x and y non units in $\mathbb{Z}[\sqrt{13}]$, as $N(2) = 4$, we must have that $N(x) = \pm 2$. Then writing $x = r + s\sqrt{3}$, we have $N(x) = r^2 - 13s^2$, so $r^2 = \pm 2 (\text{mod } 13)$ which is impossible.

So 2 is irreducible in $\mathbb{Z}[\sqrt{13}]$.

Exercise 4:
For p a prime number, the set $G = \mathbb{Z}_p^* \times \mathbb{Z}_p$ is a group for the operation:

$$(a, b) \cdot (c, d) = (ac, ad + b)$$

.
Show that $N = \{(1, x) \ / x \in \mathbb{Z}_p\}$ is a p-Sylow subgroup of G.

G has order $p(p-1)$, so any subgroup of G of order p is a p-Sylow subgroup of G. N clearly has cardinal p, so we need only to prove that it is a subgroup. We have:

- $(1, 0) \in N$, so N is non-empty
- If $(1, x)$ and $(1, y) \in N$, then $(1, x)(1, y) = (1, x + y) \in N$.
- The inverse $(1, -x)(1, x) = (1, 0)$, the inverse $(1, -x)$ of $(1, x)$ is in N.

So N is a p-Sylow subgroup of G.

Problem 1:
For this exercise, you can use the fact that $\mathbb{Z}[\sqrt{2}]$ is a Euclidian domain.
We want to compute the degree of the splitting field of $P(X) = (X^2 - 1)^2 - 8$ over $\mathbb{Q}$.

1) Find the roots of P.

$P(X) = 0 \Leftrightarrow X^2 - 1 = \pm 2\sqrt{2} \Leftrightarrow X^2 = 1 \pm 2\sqrt{2} \Leftrightarrow X = \pm\sqrt{1 \pm 2\sqrt{2}}$

2) Show that $1 + 2\sqrt{2}$ is irreducible in $\mathbb{Z}[\sqrt{2}]$

$N(1 + 2\sqrt{2}) = 1 - 2 \cdot 2^2 = -7$ is plus or minus a prime, so $1 + 2\sqrt{2}$ is irreducible in $\mathbb{Z}[\sqrt{2}]$.

3) Deduce from this that $x^2 = 1 + 2\sqrt{2}$ has no solution in $\mathbb{Q}(\sqrt{2})$
(*Hint: Use the decomposition into irreducibles in* $\mathbb{Z}[\sqrt{2}]$)

Let x in $\mathbb{Q}(\sqrt{2})$ such that $x^2 = 1 + 2\sqrt{2}$. We can always write $x = \frac{y}{z}$ where $y, z \in \mathbb{Z}[\sqrt{2}]$. Then we get

$$y^2 = z^2(1 + 2\sqrt{2})$$

If we decompose both side of the equation into a product of irreducible in $\mathbb{Z}[\sqrt{2}]$, there will be an even power of the irreducible $1 + 2\sqrt{2}$ on the left and an odd power on the right. As $\mathbb{Z}[\sqrt{2}]$ is a unique factorization domain, this is a contradiction.

4) Conclude from question 3) that $[\mathbb{Q}(\sqrt{1 + 2\sqrt{2}}) \ : \ \mathbb{Q}] = 4$.

$\sqrt{1 + 2\sqrt{2}}$ is a root of the polynomial $P(X) = X^2 - (1 + 2\sqrt{2}) \in \mathbb{Q}(\sqrt{2})[X]$. So the degree is less than 2.
As $\sqrt{1 + 2\sqrt{2}} \notin \mathbb{Q}(\sqrt{2})$ by question 3), the degree is exactly 2.

5) Show that $[\mathbb{Q}(\sqrt{1 + 2\sqrt{2}}, \sqrt{1 - 2\sqrt{2}}) \ : \ \mathbb{Q}] = 8$.

$\sqrt{1-2\sqrt{2}}$ is a root of the polynomial $Q(X) = X^2 - (1-2\sqrt{2})$ which has coefficients in $\mathbb{Q}(\sqrt{2})$, thus also in $\mathbb{Q}(\sqrt{1+2\sqrt{2}})$.

So the degree $[\mathbb{Q}(\sqrt{1+2\sqrt{2}}, \sqrt{1-2\sqrt{2}}) \ : \ \mathbb{Q}(\sqrt{1+2\sqrt{2}})]$ is less than 2.

But $\mathbb{Q}(\sqrt{1+2\sqrt{2}}) \subset \mathbb{R}$ and $\sqrt{1-2\sqrt{2}} \notin \mathbb{R}$ as $1-2\sqrt{2} < 0$.

Thus the degree $[\mathbb{Q}(\sqrt{1+2\sqrt{2}}, \sqrt{1-2\sqrt{2}}) \ : \ \mathbb{Q}(\sqrt{1+2\sqrt{2}})]$ is exactly 2, and by 4)

$$[\mathbb{Q}(\sqrt{1+2\sqrt{2}}, \sqrt{1-2\sqrt{2}}) \ : \ \mathbb{Q}] = 8$$

Problem 2:
We are interested in the equation

$$(E_D): \quad x^2 - 3y^2 = D$$

where x and y are integers and $D \in \mathbb{Z}$ non-zero is a parameter.

1) Show the equation (E_D) is equivalent to $N(z) = D$ where $z = x + y\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ and N is the norm.
Show also that $x = 2$,$y = 1$ is a solution of (E_1) and find a solution of (E_{-1}).

The subject contained a mistake: there is no solution to (E_{-1})**.**

If $z = x + y\sqrt{3}$ then $N(z) = x^2 - 3y^2$, so (E_D) is equivalent to $N(z) = D$.

We have that $N(2+\sqrt{3}) = 2^2 - 3 \cdot 1^2 = 1$, so $x = 2, y = 1$ is a solution of (E_1).
If $x \in \mathbb{Z}$, then $x^2 = 0, \text{ or } 1 (\text{mod } 3)$, so there can not be any solution to (E_{-1}).

2) Considering powers $(2+\sqrt{3})^n$, show for any $D \neq 0$, there is either no solution or a infinite number of solutions.

Let z_0 be a solution of (E_D). Then $N((2+\sqrt{3})^n z_0) = N(2+\sqrt{3})^n N(z_0) = 1^n \cdot D = D$.
So if there is a solution to (E_D), there is an infinite number of them.

3) Let p be a prime. Show that p is irreducible in $\mathbb{Z}[\sqrt{3}]$ if and only if (E_p) has no solution.

In $\mathbb{Z}[\sqrt{3}]$, we have $N(p) = p^2$. If p is reducible and x is a non-unit non-associate divisor of p, we must have $N(x) = p$, which means that (E_p) has a solution.
On the other hand, if (E_p) has a solution $z = x + y\sqrt{3}$ then p is reducible as

$$p = N(z) = (x + y\sqrt{3})(x - y\sqrt{3})$$

4) We admit that $\mathbb{Z}[\sqrt{3}]$ is a principal ideal domain. Let p be a prime greater or equal to 5. Show that (E_p) has a solution if and only if $t^2 = 3 \pmod{p}$ has a solution.

(*Hint: If there is a solution to* $t^2 = 3 \pmod{p}$*, find* x *and* y *such that*

$$(x + y\sqrt{3})(x - y\sqrt{3}) = np$$

where $|n| < p$*, then show that the ideal* (p) *is not prime.*)

If $x^2 - 3y^2 = p$, then p divides neither x nor y, and $x^2 - 3y^2 = 0 (\text{mod } p)$, and thus $(x/y)^2 = 3(\text{mod } p)$.

On the other hand, if $t^2 = 3(\text{mod } p)$, then $N(t + \sqrt{3}) = 0(\text{mod } p)$. Choosing t such that $|t| \leq \dfrac{p-1}{2}$, we have $(t + \sqrt{3})(t - \sqrt{3}) = np$ with $|n| \leq p$. This implies that the ideal (p) is not prime, and thus that p is not irreducible, as $\mathbb{Z}[\sqrt{3}]$ is an principal ideal domain.