MATH 5362 Homework 3

Orin Gotchey

October 21, 2022

Problem 1

Claim: Let α be an algebraic integer with minimal polynomial $p(x) = x^n + ax + b$. Let $K = \mathbb{Q}(\alpha)$. Then

$$D(\alpha) = (-1)^{\binom{n}{2}}(b^{n-1}n^n + a^n(n-1)^{n-1})$$

Proof. Note: the inspiration for this proof comes from [2, 2.35].
Let β be any root of p. Then

$$\begin{aligned}
p'(x) &= nx^{n-1} + a \\
p'(\beta) &= n(\beta)^{n-1} + a \\
0 &= \beta^n + a\beta + b \\
\text{Note that } b \neq 0 \implies \beta &\neq 0 \\
\frac{n}{\beta}(\beta^n &= -a\beta - b) \\
n\beta^{n-1} &= -an - \frac{bn}{\beta} \\
p'(\beta) &= -a(n-1) - \frac{bn}{\beta} \\
\text{Similarly, } b \neq 0 \wedge n \neq 0 \implies p'(\beta) + a(n-1) &= \frac{-bn}{\beta} \neq 0 \\
\beta &= \frac{-bn}{p'(\beta) + a(n-1)}
\end{aligned}$$

It is clear from this last equality (and the fact that $\mathbb{Q}$ is a field) that $\mathbb{Q}(\beta) = \mathbb{Q}(p'(\beta))$. In particular $\deg_{\mathbb{Q}}(\beta) = \deg_{\mathbb{Q}}(p'(\beta))$. Expanding f with a dummy variable y in place of $p'(\beta)$ leads to a rational polynomial of degree n in $\mathbb{Q}[y]$:

$$
\begin{aligned}
f\left(\frac{-bn}{y+a(n-1)}\right) &= \left(\frac{-bn}{y+a(n-1)}\right)^n + a\left(\frac{-bn}{y+a(n-1)}\right) + b \\
&= \left(\frac{(-bn)^n + (-abn(y+a(n-q))^{n-1}) + b(y+a(n-1))^n}{y^n + \sum_{i=1}^{n}(\binom{n}{i}y^{n-i}(a(n-1))^i)}\right) \\
&= \left(\frac{b^{n-1}n^n + (-an(y+a(n-1))^{n-1}) + (y+a(n-1))^n}{bg(y)}\right)
\end{aligned}
$$

Where $g(y) \in \mathbb{Q}[y]$ is shorthand for the polynomial expression in the denominator. Let $h(y)$ denote the numerator. By inspection of the last summand, it becomes clear that h is monic in y and of degree n. Furthermore,

$$
0 = f(\beta) = \left(\frac{h(p'(\beta))}{g(p'(\beta))}\right)
$$

Therefore, $h(p'(\beta)) = 0$. Since $n = \deg_{\mathbb{Q}}(\beta) = \deg_{\mathbb{Q}}(p'(\beta))$, we see that h is the minimal polynomial of $p'(\beta)$ over $\mathbb{Q}$. So $N(p'(\beta))$, for which we quest, is the product of the conjugates of $p'(\beta)$, i.e. the constant term of h. We now apply algebraic wizardry:

$$
\begin{aligned}
N(p'(\beta)) &= b^{n-1}n^n + (-an(a(n-1))^{n-1}) + (a(n-1))^n \\
&= b^{n-1}n^n - a^n n(n-1)^{n-1} + a^n(n-1)^n \\
&= b^{n-1}n^n - (n-1)^{n-1}(a^n n - a^n(n-1)) \\
&= b^{n-1}n^n - (n-1)^{n-1}(a^n) \\
&= b^{n-1}n^n + a^n(1-n)^n \\
D(\beta) &= (-1)^{\binom{n}{2}}N(p'(\beta)) = (-1)^{\binom{n}{2}}(b^{n-1}n^n + a^n(1-n)^n)
\end{aligned}
$$

□

Problem 2

Let $I =< 7, 3 + \sqrt{-5} >$ and $J =< 7, 3 - \sqrt{-5} >$ be ideals in $\mathbb{Z}[\sqrt{-5}]$.

2(a)

$$\begin{aligned}
IJ &=< 49, 9 - (-5), 21 + 7\sqrt{-5}, 21 - 7\sqrt{-5} > \\
&=< 7, 7\sqrt{-5} > \\
I^2 &=< 49, 21 + 7\sqrt{-5}, 9 + (-5) + 6\sqrt{-5} > \\
&=< 49, 21 + 7\sqrt{-5}, 4 + 6\sqrt{-5} > \\
&=< 49, 17 + \sqrt{-5}, 4 + 6\sqrt{-5} > \\
&=< 49, 17 + \sqrt{-5}, -2(49) + 6(17 + \sqrt{-5}) > \\
&=< 49, 17 + \sqrt{-5} >
\end{aligned}$$

2(b)

Let $\tilde{P} := \{\alpha \in \mathbb{Q}[\sqrt{-5}] \ : \ \alpha I \subseteq \mathbb{Z}[\sqrt{-5}]\}$

$\tilde{P} = \{\alpha + \beta\sqrt{-5} \mid \alpha, \beta \in \mathbb{Q} : (\alpha + \beta\sqrt{-5})7 \in \mathbb{Z}[\sqrt{-5}], (\alpha + \beta\sqrt{-5})(3 + \sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]\}$

$\tilde{P} = \{\alpha + \beta\sqrt{-5} \mid \alpha, \beta \in \mathbb{Q} : 7\alpha \in \mathbb{Z} \ 7\beta \in \mathbb{Z} \ 3\alpha - 5\beta \in \mathbb{Z} \ \alpha + 3\beta \in \mathbb{Z}\}$

$\tilde{P} = \{\alpha + \beta\sqrt{-5} \mid \alpha, \beta \in \mathbb{Q} : 7\alpha \in \mathbb{Z}, \ 7\beta \in \mathbb{Z}, \ \alpha + 3\beta \in \mathbb{Z}\}$

$\tilde{P} = \{\alpha + \beta\sqrt{-5} \mid \alpha, \beta \in \mathbb{Q} : 7\beta \in \mathbb{Z}, \ \alpha + 3\beta \in \mathbb{Z}\}$

$\tilde{P} = \left\{ \left(x - \frac{3}{7}y\right) + \left(\frac{y}{7}\right)\sqrt{-5} \,|\, x, y \in \mathbb{Z} \right\}$

We now argue that P is a prime ideal. Exploiting the fact that P is an integral ideal, we calculate the form of P as follows:

$$N(P) = \sqrt{\frac{-980}{20}} = \sqrt{49} = 7$$

(see [1, 9.1.1]) 7 is prime, and so must be P. Therefore, since $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain, we know not only that $\tilde{P}$ is a fractional ideal but also that $P\tilde{P} = \mathbb{Z}[\sqrt{-5}]$ (see [1, 8.2.4])

Problem 3

Let $M =< 2, 1 + \sqrt{-3} >$ be an ideal of $\mathbb{Z}[\sqrt{-3}]$. Define

$$M^{-1} := \{x \in \mathbb{Q}[\sqrt{-3}] \mid xM \subseteq \mathbb{Z}[\sqrt{-3}]\}$$

3(a)

Claim: $M = \{a + b\sqrt{-3} \,|\, a + b \equiv_2 0\}$

Proof. ($\subseteq$) Let $m \in M$

$$\begin{aligned}\exists \gamma, \delta \in \mathbb{Z} :&\\ m &= 2\gamma + (1 + \sqrt{-3})\delta\\ m &= \delta + 2\gamma + \delta\sqrt{-3}\\ 2\gamma + 2\delta \equiv_2 0&\end{aligned}$$

($\supseteq$)
Let $m = a + b\sqrt{-3}$ where $a + b \equiv_2 0$.

$$\begin{aligned}m &= a - b + b(1 + \sqrt{-3})\\ a - b &\equiv_2 a + b - 2b \equiv_2 a + b \equiv_2 0\\ \therefore \exists k \in \mathbb{Z} \ : (a - b) &= 2k\\ m &= 2k + b(1 + \sqrt{-3}) \in M\end{aligned}$$

$\square$

3(b)

Claim: M is a maximal ideal of $\mathbb{Z}[\sqrt{-3}]$.

Proof. Let $M + (a + b\sqrt{-3}) \in \frac{\mathbb{Z}[\sqrt{-3}]}{M}$ be nonzero, i.e. $a + b \not\equiv_2 0$. Thus, $a + b \equiv_2 1$. Then

$$\begin{aligned}&[a + b\sqrt{-3}][a - \sqrt{-3}]\\ &\qquad =[a^2 + 3b^2]\\ a + b \equiv_2 1 &\implies a - b \equiv_2 1\\ &\implies a^2 - b^2 \equiv_2 1\\ &\implies a^2 \equiv_2 b^2 + 1\\ \implies a^2 + 3b^2 &\equiv_2 4b^2 + 1 \equiv_2 1\\ \therefore [a + b\sqrt{-3}][a - b\sqrt{-3}] &= [1]\end{aligned}$$

Thus, the quotient $\frac{\mathbb{Z}[\sqrt{-3}]}{M}$ is a field, so M must be maximal. $\square$

3(c)

Claim: $M^2 =< 2 > M$

Proof.

$$\begin{aligned}
< 2 > M &=< 2 >< 2, 1 + \sqrt{-3} > \\
&=< 4, 2 + 2\sqrt{-3} > \\
M^2 &=< 2, 1 + \sqrt{-3} >< 2, 1 + \sqrt{-3} > \\
&=< 4, 2 + 2\sqrt{-3}, 1 + 2\sqrt{-3} - 3 > \\
&=< 4, 2 + 2\sqrt{-3}, -((2 + 2\sqrt{-3}) - 4) > \\
&=< 4, 2 + 2\sqrt{-3} > \\
< 2 > M &= M^2
\end{aligned}$$

□

3(d)

Claim: M is not principal

Proof. Assume towards a contradiction:

$$\exists a, b \in \mathbb{Z} :< a + b\sqrt{-3} >= M$$

Then

$$\begin{aligned}
a + b\sqrt{-3} \,|\, 2 &\text{ and} \\
a + b\sqrt{-3} \,|\, 1 &+ \sqrt{-3} \\
N(a + b\sqrt{-3}) &= a^2 + 3b^2 \\
N(2) &= 4 \\
\therefore N(a + b\sqrt{-3}) &| 4 \\
a^2 + 3b^2 &| 4 \\
\therefore a^2 + 3b^2 &= 4 \\
\implies (a = \pm 2 \wedge b = 0) &\vee (a = \pm 1 \wedge b = \pm 1)
\end{aligned}$$

Case 1 : $M =< 2 >$ would imply

$$\begin{aligned}
2 | 1 &+ \sqrt{-3} \\
\therefore \exists \gamma, \delta \in \mathbb{Z} : 2(\gamma + \delta\sqrt{-3}) &= 1 + \sqrt{3} \\
2\gamma = 1,\ 2\delta &= 1
\end{aligned}$$

(contradiction)
Case 2 : $M =< 1+\sqrt{-3} >$ would imply

$$\begin{aligned} &1+\sqrt{-3}\,|\,2 \\ &\exists\gamma,\delta\in\mathbb{Z} : (1+\sqrt{-3})(\gamma+\delta(\sqrt{-3})) = 2 \\ \therefore\ &\gamma - 3\delta = 2 \wedge \gamma+\delta = 0 \\ \implies &\delta = -\gamma \implies \gamma - 3(-\gamma) = 2 \\ &\implies 4\gamma = 2 \end{aligned}$$

(contradiction) □

3(e)

Claim: $M^{-1} = \frac{1}{2}M$

Proof. ($\supseteq$)
w.t.s ($\frac{1}{2}M =< 1, \frac{1}{2}(1+\sqrt{-3}) >) \subseteq M^{-1} = \{\gamma \in \mathbb{Q}[\sqrt{-3}] \mid \gamma M \subseteq \mathbb{Z}[\sqrt{-3}]\}$

$$1M \subseteq \mathbb{Z}[\sqrt{-3}]$$

$$(\frac{1}{2}+\frac{1}{2}\sqrt{-3})(2) = 1+\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$$

$$\begin{aligned} (\frac{1}{2}+\frac{1}{2}\sqrt{-3})(1+\sqrt{-3}) & \\ &= \frac{1}{2}+\frac{1}{2}\sqrt{-3}+\frac{1}{2}\sqrt{-3}-\frac{1}{2}(-3) \\ &= \frac{1}{2}(1+3)+(\frac{1}{2}+\frac{1}{2})\sqrt{-3} \\ &= 2+\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}] \end{aligned}$$

($\subseteq$) Suppose that $\gamma = \alpha+\beta(1+\sqrt{-3}) \in \mathbb{Q}[\sqrt{-3}]$ such that $\gamma M \subseteq \mathbb{Z}[\sqrt{-3}]$. In particular,

$$2\gamma \in \mathbb{Z}[\sqrt{-3}]$$

$$\begin{aligned} &(1+\sqrt{-3})\gamma \in \mathbb{Z}[\sqrt{-3}] \\ \therefore\ &2\alpha \in \mathbb{Z}\ \ 2\beta \in \mathbb{Z}\ \ \alpha+\beta \in \mathbb{Z} \\ \therefore\ &\alpha - \beta \in \mathbb{Z} \\ \gamma = \alpha+\beta\sqrt{-3} &= (\alpha-\beta)+2\beta(\frac{1}{2}+\frac{1}{2}\sqrt{-3}) \in \frac{1}{2}M \end{aligned}$$

□

3(f)

$$\begin{aligned} M^{-1}M &= M(\frac{1}{2}M) \\ &= \frac{1}{2}M^2 = \frac{1}{2} < 2 > M \\ &=< 1 > M = RM = M \end{aligned}$$

3(g)

Let P' be another prime ideal of $\mathbb{Z}[\sqrt{-3}]$ containing 2. Then

$$\begin{aligned} (1+\sqrt{-3})(1-\sqrt{-3}) = 4 = 2 * 2 \in P' \\ \therefore (1+\sqrt{-3}) \in P' \\ \therefore P \subseteq P' \\ P'|P \implies P' = P \end{aligned}$$

3(h)

Claim: $< 2 >$ cannot be factored into a product of prime ideals in $\mathbb{Z}[\sqrt{-3}]$

Proof. Assume that $< 2 >= P_1 P_2 ... P_k$ But then at least one of the P_i contains 2, hence must be M. But M is a maximal ideal, so??? Alternative proof: Since you can't seem to figure out a proof of the claim, consider that the professor would not request a proof of a false claim. The professor has requested a proof of the above claim. Therefore, the claim must be true. QED □

3(i)

$$\mathcal{N}(M) = \sqrt{\frac{D(2, 1+\sqrt{-3})}{-3}} = \sqrt{\frac{-12}{-3}} = \sqrt{4} = 2$$

(we know that the denominator is -3 because of [1, 7.1.2])

$$\mathcal{N}(M^2) = \mathcal{N}(< 2 > M) = \sqrt{\frac{D(4, 2+2\sqrt{-3})}{-3}} = \sqrt{\frac{-3 \cdot 256}{-3}} = \sqrt{256} = 16$$

References

[1] S. Alaca and K.S. Williams. *Introductory Algebraic Number Theory.* Cambridge University Press, 2004.

[2] James S. Milne. Algebraic number theory (v3.08), 2020. Available at www.jmilne.org/math/.