Math 562 Homework 3 — Spring 2012, Drew Armstrong

Problems on Number Theory

The first problem substitutes for the proof of FLT(3), which was too hard.

1. Prove that the equation $y^3 = x^2 + 2$ has exactly two integer solutions: $(x, y) = (\pm 5, 3)$.

(a) If $y^3 = x^2 + 2$ is an integer solution, show that x is odd. [Hint: Reduce mod 4.]

(b) If x is odd, show that $x + \sqrt{-2}$ and $x - \sqrt{-2}$ are coprime in $\mathbb{Z}[\sqrt{-2}]$. [Hint: If α is a common divisor then α divides the sum $2x$ and the difference $2\sqrt{-2}$. Taking norms gives $N(\alpha)|4x^2$ and $N(\alpha)|8$, hence $N(\alpha)|4$. Show that α must be ± 1.]

(c) If $y^3 = x^2 + 2$ is an integer solution then we have $y^3 = (x + \sqrt{-2})(x - \sqrt{-2})$. Use part (b) and the fact that $\mathbb{Z}[\sqrt{-2}]$ is a UFD (proved on the last homework) to conclude that $x + \sqrt{-2} = (a + b\sqrt{-2})^3$ for some $a, b \in \mathbb{Z}$. [Hint: The units of $\mathbb{Z}[\sqrt{-2}]$ are ± 1.]

(d) If $y^3 = x^2+2$ and $(x+\sqrt{-2}) = (a+b\sqrt{-2})^3$, show that $(a, b) = (\pm 1, 1)$, hence $(x, y) = (\pm 5, 3)$.

Proof. Suppose that $y^3 = x^2 + 2$ with $x, y \in \mathbb{Z}$. We wish to show that $(x, y) = (\pm 5, 3)$. If x is even then $x^2 = 0$ mod 4. But then $y^3 = 2$ mod 4, which has no solution, hence x is odd.

Next suppose that $\alpha = a + \sqrt{-2}$ is a common divisor of $x + \sqrt{-2}$ and $x - \sqrt{-2}$. Since the norm is multiplicative this implies that $N(\alpha)$ divides $N(x \pm \sqrt{-2}) = x^2 + 2$ as integers. We also know that α divides $(x + \sqrt{-2}) - (x - \sqrt{-2}) = 2\sqrt{-2}$ and hence $N(\alpha)$ divides $N(2\sqrt{-2}) = 8$ as integers. Since

We conclude that $N(\alpha) = a^2 + 2b^2 = 1$ and hence $\alpha = \pm$. That is, $x \pm \sqrt{-2}$ are coprime elements of $\mathbb{Z}[\sqrt{-2}]$.

We can factor $y^3 = (x + \sqrt{-2})(x - \sqrt{-2})$ in the ring $\mathbb{Z}[\sqrt{-2}]$. Note that the prime factors of y^3 come in threes. Then since $\mathbb{Z}[\sqrt{-2}]$ is a UFD and since $x \pm \sqrt{-2}$ are coprime, the prime factors of $x + \sqrt{-2}$ must also come in threes. In other words, we have $x + \sqrt{-2} = u(a + b\sqrt{-2})^3$ where $u \in \mathbb{Z}[\sqrt{-2}]$ is a unit and $a, b \in \mathbb{Z}$. Since the units of $\mathbb{Z}[\sqrt{-2}]$ are ± 1, we can just say that $x + \sqrt{-2} = (a + b\sqrt{-2})^3$ for some $a, b \in \mathbb{Z}$.

Thus we have

$$x + \sqrt{-2} = a^3 + 3a^2b\sqrt{-2} + 3a(b\sqrt{-2})^2 + (b\sqrt{-2})^3 = (a^3 - 6ab) + (3a^2b - 2b)\sqrt{-2}.$$

Comparing coefficients gives $x = a^3 - 6ab = a(a^2 - 6b)$ and $1 = 3a^2b - 2b^3 = b(3a^2 - 2b^2)$. The second equation requires $(a, b) = (\pm 1, 1)$, which then implies that $x = \pm 5$. Finally we have $y^3 = x^2 + 2 = 27$ which implies $y = 3$. We conclude that $(x, y) = (\pm 5, 3)$. $\square$

[This result is attributed to Euler (1770), and explains why number theorists care about UFDs. I promise that I won't make you do any more Diophantine equations.]

2. Recall that the product of ideals $I, J \subseteq R$ is given by $IJ := (\{uv : u \in I, v \in J\})$. Given the **non-principal** ideal $A = (2) + (1 + \sqrt{-5}) = (2, 1 + \sqrt{-5}) \subseteq \mathbb{Z}[\sqrt{-5}]$ and its conjugate $\bar{A} = (2, 1 - \sqrt{-5})$, prove that $A\bar{A} = (2)$ (which is principal).

Proof. First note that $2 \in A\bar{A}$ because $2 = 6 - 4 = (1 + \sqrt{-5})(1 - \sqrt{-5}) - 2 \cdot 2$. Since $A\bar{A}$ is an ideal this implies $(2) \subseteq A\bar{A}$. Conversely, note that the general element of $A\bar{A}$ look like

$$\begin{aligned}(2a + (1 + \sqrt{-5})b)(2c + (1 - \sqrt{-5})d) &= 4ac + 2(1 - \sqrt{-5})ad + 2(1 + \sqrt{-5})bc + 6bd \\ &= 2[(2ac + ad + bc + 3bd) + (bc - ad)\sqrt{-5}].\end{aligned}$$

Since this is divisible by 2 in $\mathbb{Z}[\sqrt{-5}]$ we get $A\bar{A} \subseteq (2)$. $\square$

[It's a general fact that for any ideal $I \subseteq \mathbb{Z}[\sqrt{-5}]$ we have $I\bar{I} = (n)$ for some $n \in \mathbb{Z}$ and this is exactly what's needed to prove that $\mathbb{Z}[\sqrt{-5}]$ has unique factorization of ideals.]

Problems on Polynomials

3. Consider the ring of polynomials $R[x]$ with coefficients in an integral domain R.

(a) Prove that $R[x]$ is an integral domain.

(b) Prove that for all $f, g \in R[x]$ with $fg \neq 0$ we have $\deg(fg) = \deg(f) + \deg(g)$. If you want the statement to remain true for $fg = 0$ how should you define $\deg(0)$?

(c) We can identify $R \subseteq R[x]$ as the constant polynomials. Prove that $R[x]^\times = R^\times$.

Proof. Note that a polynomial in $R[x]$ is zero if and only if its leading coefficient is zero. Consider $f(x) \neq 0$ and $g(x) \neq 0$ in $R[x]$ with leading coefficients $a \neq 0$ and $b \neq 0$, respectively. Then $f(x)g(x)$ has leading coefficient $ab \neq 0$, hence $f(x)g(x) \neq 0$. We conclude that $R[x]$ is an integral domain. Next suppose that $f(x)$ and $g(x)$ have leading terms ax^m and bx^n, respectively. Then the leading term of $f(x)g(x)$ is $ax^m bx^n = abx^{m+n}$, which is nonzero since $a, b \neq 0$. We conclude that $\deg(fg) = m + n = \deg(f) + \deg(g)$. What if $fg = 0$? Without loss of generality this implies that $f = 0$. How could we define $\deg(0)$ so that the equation $\deg(0) = \deg(0) + \deg(g)$ is true for all g? Answer: $\deg(0) = -\infty$. Or you could just avoid defining $\deg(0)$ at all. Finally, we will show that $R[x]^\times = R^\times$. First note that $R^\times \subseteq R[x]^\times$ since if $ab = 1$ in R, then $ab = 1$ in $R[x]$ also. Conversely, suppose that $f \in R[x]^\times$ so there exists $g \in R[x]$ with $fg = 1$. Applying the degree map gives $\deg(fg) = \deg(f) + \deg(g) = \deg(1) = 0$. Since $\deg(f), \deg(g)$ are non-negative integers this implies $\deg(f) = \deg(g) = 0$. In other words, $f, g \in R^\times$. Hence $R[x]^\times \subseteq R^\times$. $\square$

4. If R is not an integral domain then $(R[x])^\times$ will be bigger than $R^\times$. In particular, if $a \in R$ is nilpotent (say $a^n = 0$), prove that $1 + ax \in R[x]$ is a unit. [Hint: You can write $1 = 1 + a^n x^n$.] Find the inverse of $1 + 3x$ in $\mathbb{Z}/(27)[x]$.

Proof. We have $1 = 1 + a^n x^n = (1 + ax)(1 - ax + a^2x^2 - \cdots + (-1)^{n-1}a^{n-1}x^{n-1})$. Hence the inverse of $1 + 3x$ in $\mathbb{Z}/(27)[x]$ is $1 - 3x + 9x^2$. (Check: $(1 + 3x)(1 - 3x + 9x^2) = 1 + 27x^3 = 1$.) $\square$

[The general theorem says that $f(x) = \sum a_i x^i \in R[x]$ is a unit if and only if $a_0 \in R^\times$ and a_i is nilpotent for all $i \geq 1$. Give it a try if you want.]

Problems on Fields

5. We say that an ideal $I \subseteq R$ is maximal if there does **not** exist an ideal $J \subseteq R$ with $I < J < R$. Prove that $I \subseteq R$ is maximal if and only if R/I is a field. Describe the maximal ideals of a PID.

Proof. I will give two proofs. First the fancy proof. By the correspondence theorem there is a 1-1 correspondence between nontrivial ideals of R/I and ideals strictly between I and R. Note that R/I is a field if and only if it has no nontrivial ideals (proved on the first homework) if and only if there are no ideals strictly between I and R if and only if I is maximal.

Now an explicit proof. Let $I \subseteq R$ be maximal and consider an element $a + I \in R/I$. If $a + I \neq 0 + I$ then $a \notin I$. But then the ideal $(a) + I$ is strictly larger than I. By maximality of I this implies that $(a) + I = R$. Since $1 \in R = (a) + I$, there exist $b \in R$ and $u \in I$ such that $1 = ab + u$. But then $(a + I)(b + I) = ab + I = 1 - u + I = 1 + I$. Hence $(a + I)^{-1} = (b + I)$ and R/I is a field.

Conversely, suppose that R/I is a field and let $\varphi : R \to R/I$ be the natural map. If $J \subseteq R$ is an ideal with $I < J$ then $\varphi(J)$ is a nonzero ideal of R/I. (Proof: Consider $(u + I), (v + I) \in \varphi(J)$ and $(a + I) \in R/I$. Then we have $(u + I) + (a + I)(v + I) = (u + av) + I \in \varphi(J)$ because $u + av \in J$. The ideal $\varphi(J)$ is nonzero because it contains $\varphi(a)$ for some $a \in J$ but not in $I = \ker \varphi$.) But you showed on the first homework that the only nonzero ideal of a field is the field itself, hence

$\varphi(J) = R/I$. Now since $1 + I \in \varphi(J) = R/I$, there exists $a \in J$ such that $\varphi(a) = 1 + I$, and then $\varphi(1-a) = \varphi(1) - \varphi(a) = (1+I) - (1+I) = 0 + I$ implies that $1 - a \in \ker\varphi = I < J$. Since J is an ideal this implies $1 = a + (1-a) \in J$ and hence $J = R$ (you showed on the first homework that any ideal containing a unit is the full ring). We conclude that I is maximal.

In a PID, note that $(a) \subseteq R$ is maximal if and only if the element $a \in R$ is irreducible. And since a PID is a domain, this happens if and only if $a \in R$ is prime. $\square$

6. Let $\gamma \in \mathbb{C}$ be a root of the polynomial $f(x) = x^3 - 2$.

(a) Prove that $f(x)$ is irreducible over $\mathbb{Q}$ and hence $\mathbb{Q}[x]/(f) \approx \mathbb{Q}(\gamma)$ is a field.

(b) Compute the inverse of $1+2\gamma+\gamma^2$ in $\mathbb{Q}(\gamma)$. [Hint: Apply the Euclidean algorithm to express 1 as a linear combination of $1 + 2x + x^2$ and $x^3 - 2$ with coefficients in $\mathbb{Q}[x]$. Plug in γ.]

Proof. If $x^3 - 2$ is reducible then it has a factor of degree 1 and by the factor theorem this implies that $x^3 - 2$ has a root in $\mathbb{Q}$, say $\delta^3 - 2 = 0$ for $\delta \in \mathbb{Q}$. Write $\delta = a/b$ with $a, b \in \mathbb{Z}$ coprime and note that $\delta^3 = 2$ implies $a^3 = 2b^3$. This implies that a^3 and hence a is even, say $a = 2k$. But then $2b^3 = a^3 = 8k^3$ implies $b^3 = 4k^3$, hence b is even. This contradicts our assumption that a, b are coprime. Hence $x^3 - 2$ is irreducible over $\mathbb{Q}$. By Problem 5 this implies that $\mathbb{Q}[x]/(x^3 - 2) \approx \mathbb{Q}(\gamma)$ is a field.

To compute the inverse of $1 + 2\gamma + \gamma^2 \in \mathbb{Q}(\gamma)$ we will express 1 as a combination of $x^2 + x + 1$ and $x^3 - 2$ in $\mathbb{Q}[x]$. First divide $x^3 - 2$ by $x^2 + 2x + 1$ to get $(x^3 - 2) = (x - 2)(x^2 + 2x + 1) + 3x$. Then divide $x^2 + 2x + 1$ by $3x$ to get $(x^2 + 2x + 1) = (x/3 + 2/3)(3x) + 1$. Finally, back-substitute:

$$\begin{aligned}
1 &= (x^2 + 2x + 1) - (x/3 + 2/3)(3x) \\
&= (x^2 + 2x + 1) - (x/3 + 2/3)[(x^3 - 2) - (x - 2)(x^2 + 2x + 1)] \\
&= [1 + (x/3 + 2/3)(x - 2)](x^2 + 2x + 1) - (x/3 + 2/3)(x^3 - 2) \\
&= (x^2/3 - 1/3)(x^2 + 2x + 1) - (x/3 + 2/3)(x^3 - 2).
\end{aligned}$$

Plugging in $x \mapsto \gamma$ gives $1 = (\gamma^2/3 - 1/3)(\gamma^2 + 2\gamma + 1)$, hence $(1 + 2\gamma + \gamma^2)^{-1} = \gamma^2/3 - 1/3$.

One could follow exactly the same procedure to compute $(a + b\gamma + c\gamma^2)^{-1}$ for general $a, b, c \in \mathbb{Q}$. I did this on my computer and got

$$(a + b\gamma + c\gamma^2)^{-1} = \left(\frac{a^2 - 2bc}{\Delta}\right) + \left(\frac{2c^2 - ab}{\Delta}\right)\gamma + \left(\frac{b^2 - ac}{\Delta}\right)\gamma^2,$$

where $\Delta = a^3 + 2b^3 + 4c^3 - 6abc$. Check that $(a, b, c) = (1, 2, 1)$ gives the right answer. (If you want to do it by hand, it's probably easier to expand $(a + b\gamma + c\gamma)(X + Y\gamma + Z\gamma^2) = 1 + 0\gamma + 0\gamma^2$ and compare coefficients of γ to get a 3×3 linear system in X, Y, Z. Then solve using Gaussian elimination.) $\square$

[Note that the three (complex) roots of $x^3 - 2$ are indistinguishable over $\mathbb{Q}$, so I chose not to say $\gamma = \sqrt[3]{2} \in \mathbb{R}$. The field $\mathbb{Q}$ doesn't really know what γ "is"; it only knows that $\gamma^3 - 2 = 0$.]