Math 562 **Spring 2012**
Homework 3 **Drew Armstrong**

Problems on Number Theory

The first problem substitutes for the proof of FLT for exponent 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 $(x, y) = (\pm 5, 3)$.

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).

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 $(R[x])^\times = R^\times$.

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 $\mathbb{Z}/(27)[x]$.

[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.

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.]

[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 $\gamma^3 - 2 = 0$.]