MATH 124 HOMEWORK #8

INNA ZAKHAREVICH

(1) We write $f(x,y) = y^2 - x^3 + 43x - 166$. Then we know that, at $(3,8)$ we have

$$\frac{\partial f}{\partial x}(3,8) = (-3x^2+43)\big|_{x=3} = 16 \qquad \frac{\partial f}{\partial y}(3,8) = (2y)|_{y=8} = 16.$$

Thus we have that the tangent line at $(3,8)$ has slope -1, and thus its equation is $y = -x + 11$. Plugging this in to f, we get

$$-x^3 + (-x+11)^2 + 43x - 166 = -x^3 + x^2 + 21x - 45 = -(x-3)^2(x+5).$$

Thus the third point of intersection of the tangent line with the curve is $(-5,16)$, so $2P = (-5,-16)$.

At $(-5,-16)$ we have

$$\frac{\partial f}{\partial x}(-5,-16) = (-3x^2+43)\big|_{x=-5} = -32 \qquad \frac{\partial f}{\partial y}(-5,-16) = (2y)|_{y=-16} = -32.$$

Thus the slope of the tangent line at $(-5,-16)$ is -1, so the equation for the line is $y = -x - 21$. Plugging this in to f we get

$$-x^3 + (x+21)^2 + 43x - 166 = -x^3 + x^2 + 85x + 275 = (x+5)^2(x-11).$$

Thus the third point of intersection of the tangent line with the curve is $(11,-32)$, so $4P = (11,32)$.

Now we just need to compute $7P = 4P + 2P + P$. Notice that if $6P = -P$ we are done, since then P must be a torsion point of order 7. The line going through $4P$ and $2P$ has equation $y = 3x - 1$. Plugging this in to f, we get

$$-x^3 + (3x-1)^2 + 43x - 166 = -x^3 + 9x^2 + 37x - 165 = (x-3)(x+5)(x-11).$$

Thus the third point of intersection of the line and the curve is $(3,8)$, so $6P = (3,-8) = -P$, as desired.

(2) (a) We define $N(f(x)) = \deg f$. We claim that for any two polynomials f, g we can find polynomials q, r such that $\deg r < \deg g$ and

$$f(x) = q(x)g(x) + r(x).$$

If we can show that given two polynomials f, g with $\deg f \geq \deg g$ we can find a polynomial h with $\deg h < \deg f$ that is a combination of f and g we are done, since repeated iteration of this will show that we can write $f(x) = q(x)g(x)+r(x)$ with $\deg r < \deg g$ (otherwise we could apply the procedure to r and get a polynomial with smaller degree).

Suppose that f has leading coefficient a and g has leading coefficient b. Then the coefficient of $x^{\deg f}$ in

$$f(x) - \frac{a}{b}x^{\deg f - \deg g}g(x)$$

is zero by construction, so the above expression has degree less than f and we are done.

(b) We will denote the norm of an element x by $N(x)$.
Suppose that R has a Euclidean algorithm. Let I be an ideal, and suppose that a is an element of minimal norm. We claim that $I = (a)$.
Suppose that we have an element $f \in I$. Since R has a Euclidean algorithm, we must have $f = qa + r$. Notice that $f - qa \in I$, since I is an ideal. Therefore $r \in I$, and so $N(r) \geq N(a)$ unless $r = 0$. But from the definition of the Euclidean algorithm, $N(r) < N(a)$, so we get that $r = 0$. Thus $f = qa$, so $f \in (a)$. Thus $I \subset (a)$. But $(a) \subset I$, since $a \in I$. Thus $I = (a)$, as desired.

(c) Suppose that $f, g \in I_\alpha$. Then $(f+g)(\alpha) = f(\alpha)+g(\alpha) = 0+0 = 0$, so $f+g \in I_\alpha$. Now suppose that g is any polynomial. $(gf)(\alpha) = g(\alpha)f(\alpha) = 0g(\alpha) = 0$, so $gf \in I_\alpha$, so I_α is an ideal.

(d) Suppose that α is algebraic over $\mathbb{Q}$. Then there is a polynomial $f \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$, so I_α is nonempty. From part (a) we know that there is a Euclidean algorithm for polynomials over $\mathbb{Q}$, so we know that $I_\alpha = (f_\alpha)$. Thus for any polynomial $g \in I_\alpha$ (any polynomial such that $g(\alpha) = 0$) we must have $f_\alpha | g$, as desired.

(e) Suppose that α, α' are algebraic conjugates. Then we know that $f_\alpha = f_{\alpha'}$. Thus

$$g(\alpha) = 0 \Leftrightarrow f_\alpha | g \Leftrightarrow f_{\alpha'} | g \Leftrightarrow g(\alpha') = 0.$$

(f) Suppose that $\alpha \in \mathbb{Q}[i]$. Let f be the minimal polynomial of α. Notice that since $f \in \mathbb{Q}[x]$, $f = \bar{f}$, so its roots come in complex conjugate pairs. Thus we know that α and $\bar{\alpha}$ are both roots of f, so they are algebraic conjugates.

(g) Suppose that α is rational. Then the linear polynomial $x - \alpha \in I_\alpha$, so it is the minimal polynomial for α. Thus α has no algebraic conjugates other than itself. Now suppose that α has no algebraic conjugates other than itself. Then we know that $f_\alpha = (x - \alpha)^n$ for some n. Notice that the coefficient of x^{n-1} is $n\alpha$, which must be rational. Thus we know that $n\alpha = p/q$, so $\alpha = p/qn$, so α is rational.

(h) We know that $\sqrt[3]{2}$ is a root of the polynomial x^3-2. Thus the minimal polynomial of $\sqrt[3]{2}$ is a factor of x^3-2. If such a proper factor existed with rational coefficients, this polynomial would factor into two rational polynomials, one with degree 2 and one with degree 1, which means that it must have a rational root. However, by the rational root theorem, the denominator of the fraction must divide the leading coefficient (in a polynomial with integer coefficients); thus $x^3 - 2$ has all rational roots integers. However, this clearly has no integer roots, so it has no rational roots, so the polynomial does not factor.
Thus we know that the minimal polynomial of $\sqrt[3]{2}$ must be $x^3 - 2$, which has roots

$$\sqrt[3]{2} \qquad \frac{-1+\sqrt{3}}{2}\sqrt[3]{2} \qquad \frac{-1-\sqrt{3}}{2}\sqrt[3]{2}.$$

Thus these are the algebraic conjugates of $\sqrt[3]{2}$.

(i) Consider a rational polynomial of degree 3. This can factor into $1, 2$, or 3 factors with rational coefficients. If it factors into 1, it must have no rational roots: consider $x^3 - 2$. If it factors into 2, it must have one rational root and two complex roots. Consider the polynomial $x^3 - 1 = (x-1)(x^2+x+1)$. If it factors

into 3, it must have three rational roots (counted with multiplicity). Consider $x^3 + 3x^2 + 3x + 1 = (x + 1)^3$.