MA40188 ALGEBRAIC CURVES 2015/16 SEMESTER 1
ALGEBRA BRIEF REVIEW

This is an outline of the topics in Algebra 2B that we will review in the exercise class on 2 October. It does not mean to cover every aspect that we will need for Algebraic Curves, but I hope it will give you some help at least in the first few weeks.

Ring. A ring is a set of elements with two operations: addition and multiplication, which have to satisfy various algebraic laws. Check your Algebra 2B notes to make sure you know the full definition. We are only interested in commutative rings with 1. More precisely, we mainly focus on polynomial rings $\Bbbk[x_1, \cdots, x_n]$ and their quotient rings. (In particular, $\Bbbk[x_1, \cdots, x_n]$ can be realised as a quotient of itself by the zero ideal.)

Ideal. An ideal I is a subset of a ring R, satisfying two closedness conditions: "$a, b \in I \Longrightarrow a - b \in I$", and "$r \in R, a \in I \Longrightarrow ra \in I$". When R is a commutative ring with 1, the first condition $a - b \in I$ can be replaced by the equivalent condition $a + b \in I$.

Quotient ring. For any ideal I in a ring R, there is a quotient ring R/I, whose elements are cosets $r + I$ for any $r \in R$. Two cosets $r_1 + I$ and $r_2 + I$ are the same if and only if $r_1 - r_2 \in I$. If R is a commutative ring with 1, then so is R/I.

Ring homomorphism. A homomorphism $\varphi : R \longrightarrow S$ between two rings is a map which preserves addition and multiplication. Nice and easy.

Special rings. We have "rings $\supset$ integral domains $\supset$ UFDs $\supset$ PIDs $\supset$ fields". Make sure you know the definition of each. It is important to us that $\Bbbk[x_1, \cdots, x_n]$ is a UFD; namely, every polynomial can be factored into a product of irreducible polynomials, which is unique up to the order of factors and units (non-zero constants). It is a PID only when $n = 1$. (We now know that it is a Noetherian ring for every n.)

Polynomial. A polynomial $f(x_1, \cdots, x_n) \in \Bbbk[x_1, \cdots, x_n]$ is a finite sum of monomials. If f is not zero, then the degree of f is the highest degree of its non-zero monomials. But the degree of the zero polynomial is quite arguable. There are different ways to treat this problem. We will adopt one opinion and define the degree of the zero polynomial to be any non-negative integer. Details will be explained in week 4.

Irreducible polynomial. When $\Bbbk$ is algebraic closed, the only irreducible polynomials in $\Bbbk[x]$ are the ones of degree 1. For polynomial rings in more than 1 variable, there is no such a general rule, but irreducible polynomials can still be determined in some cases.

Example 1. We claim that $y^2 - x^3 + x \in \Bbbk[x, y]$ is an irreducible polynomial. We assume on the contrary that it can be written as the product of two non-constant factors. As a polynomial in y with coefficients in $\Bbbk[x]$, $y^2 - x^3 + x$ has degree 2 in y. Hence the two factors have degrees either 2 and 0 in y respectively, or 1 and 1 respectively. More precisely,

$$y^2 - x^3 + x = \big(f_2(x)y^2 + f_1(x)y + f_0(x)\big) \cdot g(x) \quad \text{or} \quad \big(f_1(x)y + f_0(x)\big) \cdot \big(g_1(x)y + g_0(x)\big).$$

In the first case, we have the identity $f_2(x)g(x) = 1$, hence $g(x)$ is a non-zero constant. Contradiction. In the second case, we similarly have the identity $f_1(x)g_1(x) = 1$. Therefore both factors are non-zero constants. Without loss of generality we can assume $f_1(x) = g_1(x) = 1$.

Date: October 2, 2015.

Then we have

$$y^2 - x^3 + x = (y + f_0(x))(y + g_0(x)).$$

Comparing the coefficients of y we have $f_0(x) + g_0(x) = 0$, hence $g_0(x) = -f_0(x)$. Comparing the terms without y we have $f_0(x)g_0(x) = -x^3 + x$, hence $f_0(x)^2 = x^3 - x = x(x+1)(x-1)$. The right hand side is not a square. Contradiction. This concludes that $y^2 - x^3 + x$ is an irreducible polynomial.

Algebra. You might not like the definition of a $\Bbbk$-algebra, since it is kind of long and hard to remember. We need to work with a special type of algebras called *finitely generated* $\Bbbk$*-algebras*. You might think the definition is even more involved, but it is actually very simple and explicit. A finitely generated algebra is a ring which is isomorphic to some $\Bbbk[x_1, \cdots, x_n]/I$. A $\Bbbk$*-algebra homomorphism* $\varphi : \Bbbk[x_1, \cdots, x_n]/I \longrightarrow \Bbbk[y_1, \cdots, y_m]/J$ is simply a ring homomorphism that sends a coset $c + I$ to $c + J$ for every constant c. I will formally define them in week 3.

Fundamental isomorphism theorem. The fundamental isomorphism theorem for rings is the following statement: for a ring homomorphism $f : R \longrightarrow S$, there is a canonical isomorphism

$$\operatorname{im}(f) \cong R/\ker(f).$$

This is a very important theorem for our purpose. Look at the following example.

Example 2. We claim that $\Bbbk[x,y]/(y - x^2) \cong \Bbbk[t]$. To see this, we construct a ring homomorphism (in fact, a $\Bbbk$-algebra homomorphism)

$$\varphi : \Bbbk[x,y] \longrightarrow \Bbbk[t]; \quad x \longmapsto t; \quad y \longmapsto t^2.$$

This means that every monomial ax^iy^j is sent to $at^i(t^2)^j = at^{i+2j}$, where $a \in \Bbbk$ is the coefficient. By the fundamental isomorphism theorem, we have

$$\operatorname{im}(\varphi) \cong \Bbbk[x,y]/\ker(\varphi).$$

We need to identify $\operatorname{im}(\varphi)$ and $\ker(\varphi)$.

For any $p(t) \in \Bbbk[t]$, we have $\varphi(p(x)) = p(t)$. This shows φ is surjective, hence $\operatorname{im}(\varphi) = \Bbbk[t]$.

For any $f(x,y) \in \Bbbk[x,y]$, I claim it can be written as

$$f = (y - x^2) \cdot g + h,$$

for some $g(x,y) \in \Bbbk[x,y]$ and $h(x) \in \Bbbk[x]$. For this, one only need to replace every single occurrence of y in $f(x,y)$ by $[(y - x^2) + x^2]$, and then multiply out the square brackets leaving the terms in round brackets untouched. Armed with this claim, we see that

$$\varphi(f) = \varphi(y - x^2) \cdot \varphi(g) + \varphi(h) = (t^2 - t^2) \cdot \varphi(g) + h(t) = h(t).$$

It follows that $\varphi(f) = 0 \iff h = 0 \iff f \in (y - x^2)$. Hence $\ker(\varphi) = (y - x^2)$. Therefore the fundamental isomorphism theorem implies that $\Bbbk[t] \cong \Bbbk[x,y]/(y - x^2)$.

Field. A field is a commutative ring with 1 such that every non-zero element has a multiplicative inverse. Check your Algebra 2B notes to make sure you know the *characteristic* of a field and the *field of fractions* of an integral domain (which will be used in week 6).

I strongly suggest you go through this outline to make sure you understand every item in the list as soon as possible. Otherwise you may find it more and more difficult to understand new material discussed in lectures. For your convenience, the Algebra 2B lecture notes are available on the course webpage for your reference. As always, please feel free to let me know if you have any questions.