January 18, 2013

Galois theory

1. A commutative ring $(R, 0, 1, +, \cdot)$ is an abelian group $(R, 0, +)$ together with an associative and commutative multiplication "$\cdot$" with 1 that is distributive with respect to addition: $a\cdot(b+c) = (a\cdot b)+(a\cdot c)$. For example $\mathbf{Z}$ (integers), $\mathbf{Z}/n$ (integers modulo n), $\mathbf{Q}$ rational numbers, $\mathbf{R}$ (real numbers), $\mathbf{C}$ (complex numbers).

Let R be a commutative ring. The symbol $R[X]$ denotes the polynomial ring in one variable with coefficients in R. The symbol $R[X, Y]$ denotes the polynomial ring in two variables with coefficients in R. More generally $R[X_1, \ldots, X_k]$ denotes the polynomial ring in k-variables with coefficients in R.

Let $R \subset S$ be ring and a subring. Let $s_1, \ldots, s_k$ be elements in S. The symbol $R[s_1, \ldots, s_k]$ denotes the smallest subring in S that contains R and all the elements $s_1, \ldots, s_k$. The subring $R[s_1, \ldots, s_k] \subset S$ consists of sums of elements of the form $rs_1^{l_1}s_2^{l_2}\cdots s_k^{l_k}$.

For example $\mathbf{Q}[\sqrt{5}]$ is the smallest surging of $\mathbf{R}$ that contains $\mathbf{Q}$ and $\sqrt{5}$.

An ideal in a ring is an additive subgroup $I \subset R$ such that for any a in I and any r in R, the product ra belongs to I. We say that an ideal I is generated by elements $a_1, \ldots, a_k$ if any element r in I can be written as a combination $r = r_1a_1+r_2a_2+\cdots r_ka_k$ for some elements r_i in R. If I is generated by $a_1, \ldots, a_k$, then we write $I = (a_1, \ldots, a_k)$. We say that an ideal I is principal if it is generated by only one element, i.e., if there is an element $a$in I such that all other elements in I can be written as ra for some r in R. The additive subgroup of R that consists of just the zero element 0 is an ideal. Similarly the whole ring R is also an ideal.

The the abelian group of cosets R/I with the multiplication given by $(r+I)(s+I) = rs+I$ and the element $1+I$ is a commutative ring called the quotient ring. For example $\mathbf{Z}/n$ is the quotient ring of $\mathbf{Z}$ by the ideal (n).

2. Let $R \subset S$ be ring and a subring, $f = a_0 + a_1X + \cdots + a_nX^n$ a polynomial in $R[X]$. We say that an element s in S is a zero or a solution of f is $f(s) = a_0 + a_1s + a_2s^2 + \cdots + a_ns^n = 0$. For example:

- $1 - 2x$ in $\mathbf{Z}[X]$ has no zeros in $\mathbf{Z}$ however it has a solution in rational numbers $\mathbf{Q}$ given by $1/2$.
- $2 - x^2$ in $\mathbf{Z}[X]$ has no solutions in rational numbers $\mathbf{Q}$ but it has two solutions in real numbers $\mathbf{R}$ given by $\sqrt{2}$ and $-\sqrt{2}$.
- $1 + x^2$ in $\mathbf{Z}[X]$ has no zeros in $\mathbf{R}$ but has two solutions in complex numbers $\mathbf{C}$ given by i and $-i$.
- $1+X+X^2+X^3$ in $\mathbf{Z}[X]$ has only one solution in $\mathbf{R}$ given by -1, since in $\mathbf{Z}[X]$ we have an equality $1 + X + X^2 + X^3 = (1 + X)(1 + X^2)$. It has three different solutions in $\mathbf{C}$ given by -1, i, and $-i$.
- $1+X+X^2+X^3$ in $\mathbf{Z}/2[X]$ has only one solution in $\mathbf{Z}/2$ given by 1. Note that in the ring $\mathbf{Z}/2[X]$, we have en equality $1 + X + X^2 + X^3 = (1 + x)^3$.

3**.** Let R be a ring. An element r in R is called **invertible** if there is an element $s$in R such that $rs = 1$. Such an element $s$is unique, and we call it the inverse of r and denote it by r^{-1}.

An element r is called **zero divisor** if it is not zero and there is a non-zero s such that $rs = 0$.

An element r is called **reducible**, if there are two non-invertible elements r_1 and r_2 such that $r = r_1 r_2$.

An element r is called **irreducible**, if it is not reducible, i.e., if $r = ab$, then either a or b is a unit.

An element r to divide an element s in R (denoted by $r|s$), if there a in R such that $s = ra$.

An element r is called **prime** if it is not invertible and whenever it divides a product ab, then it either devices a or it decides b.

4**. Definition.** A commutative ring is called a **domain** it it has no zero divisors. It is called a **field** if all non-zero elements are invertible. It is called a PID (principal ideal domain) if it is a domain and all its ideals are principal.

For example $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Z}[X]$, $\mathbf{Q}[X]$, $\mathbf{R}[X]$, and $\mathbf{C}[X]$, are domains. The rings $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ are fields. Any field is a domain, since whenever $a \neq 0$ and $ab = 0$, then $b = a^{-1}ab = a^{-1}0 = 0$. Moreover any field is a PID. The ring $\mathbf{Z}$ is PID. A ring $\mathbf{Z}/n$ is a domain if and only if n is a prime number. If p is a prime number, then $\mathbf{Z}/p$ is not only a domain but also a field.

5**. Proposition.** *An element r in a commutative ring R is prime if and only if r is not invertible and the quotient ring $R/(r)$ is a domain.*

For example let n be an element in $\mathbf{Z}$. Then n is a prime element in $\mathbf{Z}$ if and only if it is a prime number. Any prime number is an irreducible element in $\mathbf{Z}$.

6**. Proposition.** *Let R be a domain. Then any prime element is irreducible.*

7**. Definition.** A ring R is called UFD (unique factorization domain) if it is a domain and any element in R can be written as a product of prime elements.

8**. Proposition.** *Let R be UFD. Let p_i and q_j be prime elements in R such that $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_n$. Then $k = n$ and after a permutation, there are invertible elements u_i such that $p_i = u_i q_i$.*

Any PID is UFD. For example $\mathbf{Z}$ is a UFD and so is any field. If R is UFD, then so is the polynomial ring $R[X]$.