Notes

November 21, 2014

#8

find irreducible factors of $x^4 - 5x^2 + 6$ over $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{R}$
$\mathbb{Q}(\sqrt{2})$ is $(x - \sqrt{2})(x + \sqrt{2})(x^2 - 3)$

#14

if $m|n$ then $mk = n$ and $x^m \equiv 1 \mod x^m - 1$ and $x^{mk} \equiv 1 \mod x^m - 1$ and $x^n - 1 \equiv 0 \mod x^m - 1$
can pull out factors too
assume that $x^m - 1|x^n - 1$ then $x^n - 1 \equiv 0 \mod x^m - 1$ and $x^n = 0 \mod x^m - 1$ and $n = mq + r$ and $x^n \equiv x^r \mod x^m - 1$ and so $(x^r - 1)|(x^m - 1)$ but $r < m$ and so $r = 0$

commutative rings

what is a ring? a set (often denoted with R) with two **binary** operations (indicating closure) similar to fields. "addition" operation is abelian group, and "multiplication" is associative (and commutative when the ring is commutative) and has an identity. distribution holds. every field is a ring. rings don't require inverse for "multiplication".

examples of commutative rings

$\mathbb{Z}, \mathbb{Z}_n$, if K is a field then $K[x]$ is a commutative ring.
if R is a commutative ring, then $R[x]$ is a commutative ring.

definition

if R is a comm ring, then we say that $S \subseteq R$ is a subring if S is a comm ring on the same operations as R and has the same identity element.

example

$R \subseteq R[x]$

proposition

if $S \subseteq R$ then S is a subring iff

1. S is closed under it's operations
2. if $a \in S$ then $-a \in S$

3. $1_R \in S$ (identity in R is in S)

examples

complex integers: $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$

definition

we say the $a \in R$ is invertible if $b \in R$ such that $ab = 1_R$. another term for this is saying a is a unit, but some books call the identity a unit, so just call it invertible.

example

if $R = \{0\}$ then $1_R = 0$.
$\pm 1 \in \mathbb{Z}$ are only invertible elements in $\mathbb{Z}$

notation

$R^\times = \{x : x \in R, x \text{ is invertible}\}$
$R = \mathbb{Z}_n \to R^\times = \{[k] : \gcd(k, n) = 1\}$

proposition

if R is a commutative ring, then $(R^\times, \cdot)$ is an abelian group.

definition

an element a is called a zero divisor if there exists some $ab = 0$ where $b \neq 0$.
in $\mathbb{Z}_4$ $[2][2] = [0]$.

definition

given R a commutative ring, then we say that R is an integral domain (emphasis on integrity and domain) if $1_R \neq 0_R$ and $ab = 0$ only when $a = 0$ or $b = 0$ (that is 0_R is the only zero divisor).

example

every field is an integral domain. not that if $ab = 0$ then $a^{-1} \in F$ and $ab = a^{-1}ab = a^{-1}0 = b = 0$ and so we have a contraction if we assume $b \neq 0$.
$\mathbb{R}[x]/\langle x^2 - 1\rangle$ is not a field because x^-1 is reducible but it is a commutative ring.