Groups & Rings: Lecture #27

2016-03-21

Repetition: Rings

RINGS

- **Rings**: definitions (commutative, int. domain, field, zero divisor)
  subrings, characteristic, examples
  $R[x]$ pol. ring, matrix rings, function rings, ...
- **Homomorphisms, isomorphism theorems**
- **Ideals**: principal, prime, maximal
- **Quotient rings**: int domain, field
- **Polynomial rings**: monic, irreducible, units, evaluation homomorphism

DOMAINS

- **Factorization**: irreducible, prime
  EDs: (e.g. $\mathbb{Z}$, $F[x]$, $\mathbb{Z}[i]$) $\Rightarrow$ division algorithm
  $\Downarrow$
  PIDs: every ideal principal $\Rightarrow$ Euclid's algo for gcd
  $\Downarrow$
  UFDs: factorization into irreducibles is unique
- **Quadratic integers**: $\mathbb{Z}[\sqrt{D}] \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{D})} \subset \mathbb{Q}(\sqrt{D})$ norm
- **Irreducibility in $\mathbb{Z}[x]$ & $\mathbb{Q}[x]$**: Eisenstein's criterion, Gauss lemma
- **Fraction field**: $\mathrm{Frac}(D)$

FIELDS

- **Field extensions**: algebraic vs transcendental, prime field ($\mathbb{F}_p$ or $\mathbb{Q}$)
- **Algebraic extensions**: $F[x]/(p(x))$, minimal pol, degree, basis, finite
- **Splitting fields**: unique up to non-unique iso, algebraic closure
- **Finite fields**: separability & derivatives, Frobenius, $\exists ! \, \mathbb{F}_q$, $\mathbb{F}_q^\times$ cyclic
- **Applications**: geometric constructions, Galois theory, solvability by radicals...

Problem 2

Let R be a commutative ring with 1.

(a) ~~Define what an nilpotent element is, and~~ show that the set of nilpotent elements in R form an ideal. **(2 p)**

(b) Show that if an element $x \in R$ is nilpotent, then x is contained in any prime ideal of R. **(2 p)**

(c) Give an example of a ring R that is not an integral domain, and has no nilpotent elements other than zero. **(2 p)**

$\boxed{\text{Def: } x \in R \text{ nilpotent if } \exists n: x^n = 0}$

(a) HW4: $\{x \in R : x \text{ nilpotent}\}$ is an ideal

(i) x, y nilpotent $\Rightarrow$ $x - y$ nilpotent

(0 nilpotent, $-x$ nilpotent, $x+y$ nilpotent)

(ii) $r \in R$, x nilpotent $\Rightarrow$ rx nilpotent

(b) $x \in R$ nilpotent, $P \subset R$ prime ideal ($ab \in P \Rightarrow a \in P$ or $b \in P$)

$\Rightarrow \underbrace{x^n}_{x x^{n-1}} = 0 \in P \Rightarrow x \in P$ or $x^{n-1} \in P$

Lemma: $x^n \in P \Rightarrow x \in P$ if P prime and $n \geq 1$.

proof: Induction on n. Base case $n=1$. Arg. above gives $x \in P$

or $x^{n-1} \in P \overset{\text{induction}}{\Longrightarrow} x \in P$.

(c) non-ex: $\mathbb{Z}/(2^3)$ $\quad (\bar{2})^3 = 0$ so $\bar{2}$ nilpotent

ex: $\mathbb{Z}/(3 \cdot 5)$ $\quad \bar{3} \cdot \bar{5} = 0$ so $\bar{3}$ & $\bar{5}$ are zero-divisors

$x \in \mathbb{Z}$, $\bar{x} = 0$ in $\mathbb{Z}/15$ if $15 | x$.

$x \in \mathbb{Z}$, $\underset{3 \cdot 5}{15} \nmid x \Rightarrow 15 \nmid x^n \;\forall n$

lacks either 3 or 5

Non-ex: $\mathbb{Q}[x]/(x^n)$ $\quad \bar{x}$ nilpotent

Ex: $\mathbb{Q}[x,y]/(xy)$

Problem 4 $\boxed{2014-05-21}$

Let k be a field and consider the ring $R = k[x]/(x^2-1)$.

1. Show that the ring R is isomorphic with $k[y]/(y^2)$ if $2 = 0$ in k. (3p)
2. Show that the ring R is isomorphic with $k \times k$ if $2 \neq 0$ in k. (3p)

(1) char $k = 2$:

$$k[x]/(x^2-1) \overset{?}{\cong} k[y]/(y^2)$$

$$\{a+bx\} \qquad\qquad \{a+by\}$$

$$x \longmapsto ?$$

$$x^2 \longmapsto 1$$

Square-roots of 1 on RHS?

$$1 \overset{?}{=} (a+by)^2 = a^2 + 2aby + \cancel{b^2y^2} = a^2 + \cancel{2}aby = a^2$$

$y^2=0$ $\qquad$ $2=0$

$\Rightarrow a = \pm 1$

Evaluation homomorphisms

$$\phi : k[x] \xrightarrow{ev_{a+by}} k[y]/(y^2)$$

$$x \longmapsto a+by$$

If $a=1$, $b=1$, then $\qquad$ (Choosing $b=0 \not\Rightarrow \phi$ surj.)

- $\phi(x^2) = (a+by)^2 = a^2 = 1$
- ϕ surj b/c $\phi(1)=1$, $\phi(x-1) = y$

$\ker(\phi) \ni x^2 - 1$ Know, $k[x]$ PID

$\Rightarrow \ker(\phi) = (p(x))$

$$\left.\begin{array}{l} x - 1 \in \phi \ ? \\ x + 1 \in \phi \ ? \end{array}\right\} \underline{\text{NO}} \Rightarrow \ker\phi = (x^2 - 1)$$

1^{st} iso $\Rightarrow$ $k[x]/(x^2-1) \cong \operatorname{im}(\phi) = k[y]/(y^2)$

Problem 5 $\boxed{\text{2014-03-19}}$

Factor the polynomial $p(x) = x^4 + x + 1$ into indecomposable factors in the following rings:

1. $\mathbb{F}_2[x]$,
2. $\mathbb{F}_3[x]$,
3. $\mathbb{Q}[x]$.

In each case, argue carefully why the factors you give are indeed indecomposable.

(not on lecture)

Problem 6. (6 points). $\boxed{2015\text{-}03\text{-}16}$

Let R be the ring $\mathbb{Z}[\sqrt{-2}]$. Recall that R is a Euclidean domain with Euclidean multiplicative norm $N(a+b\sqrt{-2}) = a^2 - 2b^2$.

(a) Prove that $1 - 2\sqrt{-2}$ is a reducible element of R.

(b) Determine a greatest common divisor in R of $2 - \sqrt{-2}$ and $4 + \sqrt{-2}$.

(c) Prove that $R/(3 - \sqrt{-2})$ is a finite field with 11 elements.

$N(a+b\sqrt{D}) = (a+b\sqrt{D})(a-b\sqrt{D}) = a^2 - b^2 D$

Euclidean function for $D=-1,-2$ (book)

$|N|$ — " — $D = 2, 3$ (HW#5)

(a) $x = 1 + 2\sqrt{-2}$ reducible? (one approach: $\overset{y}{\overset{\shortparallel}{(a+b\sqrt{-2})}}\overset{z}{\overset{\shortparallel}{(c+d\sqrt{-2})}} = 1+2\sqrt{-2}$)

$x = yz$? $N(x) = N(y)N(z)$

$N(x) = 1^2 + 2\cdot 2^2 = 9 \Rightarrow N(y), N(z)$ are either

1	9
3	3
9	1

Recall: $N(y) = \pm 1 \Leftrightarrow y$ unit (easy)

$y = a + b\sqrt{-2}$ s.th. $a^2 + 2b^2 = 3 \Rightarrow a = \pm 1,\ b = \pm 1$

$(1 \pm \sqrt{-2})(1 + \sqrt{-2}) = 1 \pm (-2) + \sqrt{-2} \pm \sqrt{-2}$

$(1 - \sqrt{-2})(1 - \sqrt{-2}) = 1 + (-2) - 2\sqrt{-2} = -1 - 2\sqrt{-2}$
$= -x$

$x = \underbrace{(-1 + \sqrt{-2})}_{y}\underbrace{(1 - \sqrt{-2})}_{z}$

(b) $\gcd(2+\sqrt{-2},\ 4+\sqrt{-2}) = ?$

One solution: use Euclid's algo (b/c $\mathbb{Z}[\sqrt{-2}]$ ED)

$N(2+\sqrt{-2}) = 2^2 + 2\cdot 1^2 = 6$

$N(4+\sqrt{-2}) = 4^2 + 2\cdot 1^2 = 18$

$$4+\sqrt{-2} = \overset{\uparrow}{2}(2+\sqrt{-2}) - \underbrace{\sqrt{-2}}_{\substack{\text{remainder} \\ N = 2}}$$

guesses

$$2+\sqrt{-2} = \overset{\downarrow}{(1-\sqrt{-2})}\sqrt{-2} + 0$$

$\Rightarrow \gcd = \sqrt{-2}$

<u>Other solution</u>: gcd has norm $\underbrace{1}_{\text{units}}, \overset{\pm\sqrt{-2}}{2}, \underset{\pm 1 \pm \sqrt{-2}}{3}$ or $\overset{\pm 2 \pm \sqrt{-2}}{6}$.

Try with these.

<u>Similar problem</u>:

Problem 5 $\boxed{2014\text{-}05\text{-}21}$

Compute $\gcd(7-4\sqrt{d}, 8-\sqrt{d})$ in the ring $\mathbf{Z}[\sqrt{d}]$ for $d=-1$ and $d=-2$. (3p each)

(c) $R/(3+\sqrt{-2})$ field? 11 elements?

$\Leftrightarrow (3+\sqrt{-2})$ maximal $\Leftrightarrow$ $3+\sqrt{-2}$ irreducible

$N(3+\sqrt{-2}) = 3^2+2\cdot 1^2 = 11$ prime $\Rightarrow$ $3+\sqrt{-2}$ irreducible

($N=1 \Leftrightarrow$ unit)

$= \mathbb{F}_{11}$?

Finite field? Characteristic? $p=11$?

$\boxed{11 = 0 \text{ in } R/(3+\sqrt{-2})}$ $\Leftrightarrow$ $11+(3+\sqrt{-2}) = 0+(3+\sqrt{-2})$

$\Leftrightarrow$ $11 \in (3+\sqrt{-2})$

$\Leftrightarrow$ $3+\sqrt{-2} \mid 11$

$\Uparrow$

$11 = N(3+\sqrt{-2}) = (3+\sqrt{-2})(3-\sqrt{-2})$

Count $(a+b\sqrt{-2})$ mod $(3+\sqrt{-2})$

- $11 = 0$
- $3 = -\sqrt{2}$

} in $R/(3+\sqrt{-2})$

Every elt can be written as $\{a+b\sqrt{-2} : a\in\{0,1,2\}, b\in\{0,1,2,\dots,10\}\}$

$\Rightarrow$ at most $3\cdot 11 = 33$ elements.

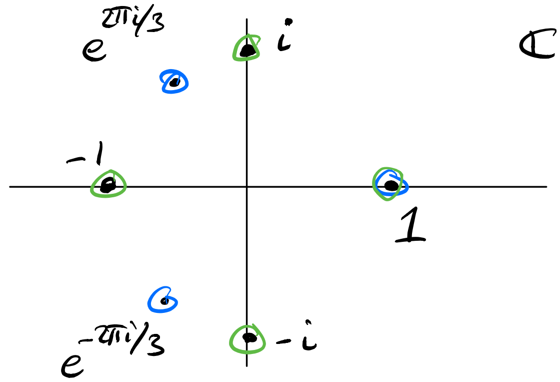
But $R/(3+\sqrt{-2})$ finite (≤ 33) field of char 11

$\Rightarrow$ has 11^n elements for some n $\Rightarrow n=1$.

Problem 4. (6 points) $\boxed{2017-03-15}$

Compute the degrees of all the field extensions of the form $\mathbb{Q} \subseteq \mathbb{Q}(\xi_1, \xi_2)$ where ξ_1 in $\mathbb{C}$ is a solution to the equation $X^3 = 1$ and ξ_2 in $\mathbb{C}$ is a solution to the equation $X^4 = 1$.

$\boxed{\xi_1^3 = 1}$, $\boxed{\xi_2^4 = 1}$ $\qquad \xi_1, \xi_2 \in \mathbb{C}$



$$\underbrace{\mathbb{Q} \subset \mathbb{Q}(\xi_1)}_{\deg\, d_1} \underbrace{\subset \mathbb{Q}(\xi_1, \xi_2)}_{\deg\, d_2} \Rightarrow \deg = d_1 d_2$$

- $\xi_1 = 1$: $\mathbb{Q} = \mathbb{Q}(\xi_1)$, $d_1 = 1$
- $\xi_1 = \pm e^{2\pi i/3}$: ξ_1 has minimal pol $x^2 + x + 1$ $\Rightarrow d_1 = 2$.

  cyclotomic pol.

- $\xi_2 = \pm 1$: $\mathbb{Q}(\xi_1) = \mathbb{Q}(\xi_1, \xi_2)$ $\Rightarrow d_2 = 1$.
- $\xi_2 = \pm i$: ξ_2 has minimal pol $x^2 + 1$ $\Rightarrow d_2 = 2$

minimal over $\mathbb{Q}$ ok

minimal over $\mathbb{Q}(\xi_1)$?

If not minimal $\Rightarrow$ x^2+1 not irr $\Rightarrow$ $x^2+1=(x+i)(x-i)$

$\Rightarrow$ $i \in \mathbb{Q}(\zeta_1)$

$\zeta_1 = e^{\pm 2\pi i/3} = -\sin 30° \pm \cos 30° i = -\frac{1}{2} \pm \frac{\sqrt{3}}{2} i$

$\mathbb{Q}(\zeta_1) = \{a + b\zeta_1 : a, b \in \mathbb{Q}\}$

$\mathrm{Re}(a+b\zeta) = 0 \Rightarrow a = \frac{1}{2} b$

$$\Rightarrow a + b\zeta_1 = \pm \underbrace{\frac{\sqrt{3}}{2}}_{\notin \mathbb{Q}} b i$$

So x^2+1 indeed irreducible over $\mathbb{Q}(\zeta_1)$ and the min. pol of ζ_2.

$\Rightarrow d_2 = 2$.

$\Rightarrow$ deg of $\mathbb{Q}(\zeta_1, \zeta_2)/\mathbb{Q}$ is either

- $1 = 1 \cdot 1$ (if $\zeta_1 = 1$, $\zeta_2 = \pm 1$)
- $2 = 2 \cdot 1 = 1 \cdot 2$ (if $\zeta_1 \neq 1$, $\zeta_2 = \pm 1$ or $\zeta_1 = 1$, $\zeta_2 = \pm i$)
- $4 = 2 \cdot 2$ (if $\zeta_1 \neq 1$, $\zeta_2 = \pm i$)