January 2020

Sunday, 26 July 2020 17:55

January 2020:

(1) - F finite field, f monic irreducible in $F[x]$, $\alpha \in \overline{F}$ root of f. Prove:

(a) $F(\alpha)$ is the splitting field for f over F.

(b) The set of roots of f is $\{\alpha^{|F|^r} \mid r \geq 1\}$.

Technique: f degree n, if $|\{\alpha^{|F|^r} \mid r \geq 1\}| = n$, and they are roots of f, we are done.

Hungerford V 1.7. We have that f is the irreducible polynomial of α and $[F(\alpha):F] = \deg(f)$.

$f(x) = a_n x^n + \cdots + a_1 x + a_0$. Now: $f(\alpha^{|F|^r}) = a_n(\alpha^{|F|^r})^n + \cdots + a_1(\alpha^{|F|^r}) + a_0 =$

$|F| = p^k$ because $|F| < \infty$

$|F| = q$

$= (a_n^{|F|^r})(\alpha^{|F|^r})^n + \cdots + (a_1^{|F|^r})(\alpha^{|F|^r}) + (a_0^{|F|^r}) =$

$= (a_n \alpha^n + \cdots + a_1\alpha + a_0)^{|F|^r} = 0.$

For all $a \in F$: $a = a^{|F|}$.

F has characteristic p.

Hence: $\{\alpha^{|F|^r} \mid r \geq 1\}$ are all roots of f. Moreover $\alpha^{|F|^r} = \alpha^{|F|^s}$ whenever $r \equiv s \mod n$,

and conversely suppose $\alpha^{|F|^r} = \alpha^{|F|^s}$, say $s = r + t$ for some $t \geq 0$. Then:

$(\alpha)^{p^{kr}} = \alpha^{|F|^r} = \alpha^{|F|^s} = \alpha^{|F|^{r+t}} = (\alpha^{|F|^t})^{|F|^r} = (\alpha^{|F|^t})^{p^{kr}} \Rightarrow \alpha = \alpha^{|F|^t}$

$a, b \in F$ field of characteristic p, if $a^p = b^p$ then $a = b$.

So α is a root of $x^{q^t} - x$ so $f(x) \mid x^{q^t} - x$ so $n \mid t$ by Exercise 5(b) August 2015 Exam.

Hence $r \equiv s \mod n$. Thus $|\{\alpha^{|F|^r} \mid r \geq 1\}| = n$, so f splits completely in $F(\alpha)$,

and these are exactly all the roots.

(2) - R local whenever R has a unique maximal ideal. Prove R local iff for all $r, r' \in R$ if $r + r' = 1$ then r or r' is a unit.

$\Rightarrow$) Suppose R local, let $r, r' \in R$ with $r + r' = 1$. Suppose that r, r' are non units, for contradiction.

Let M be the unique maximal ideal of R. Now: $(r), (r')$ are ideals of R, so $(r), (r') \subseteq M$ because every ideal is contained in a maximal ideal. $(r), (r') \subsetneq R$ However: $1 = r + r' \in (r) + (r') \subseteq M$

whence $R = (1) \subseteq M \subsetneq R$, a contradiction.

$\Leftarrow$) We prove the contrapositive. Suppose R is not local, that is, R has more than one maximal ideal.

Let M, M' be two distinct maximal ideals of R. Then $R = M + M'$, which means that

$1 = r + r'$ for some non-units $r, r' \in R$ and $r \in M$, $r' \in M'$.

Useful facts about local rings:

(i) A ring (with unit) is local iff the set of non-unit elements is an ideal.

Useful facts about local rings:

(i) A ring (with unit) is local iff the set of non-unit elements is an ideal.

(ii) Let R ring with unit, $M \subseteq R$ maximal ideal. If every element of $1+M$ is a unit, then R local.