July 23

Thursday, July 23, 2020 10:40 AM

August 2016:

(1) - Let G group, $|G| = 140$, prove G has a cyclic normal subgroup of order 35.

$|G| = 140 = 2^2 \cdot 5 \cdot 7$, by the 3rd Sylow Theorem: $\underset{H_5}{n_5 = 1}$, $\underset{H_7}{n_7 = 1}$. } details

Since $\gcd(5,7) = 1$, H_5 and H_7 cannot have nontrivial intersection: $H_5 \cap H_7 = \{e\}$.
details

$|H_5 \times H_7| = 35$, so we only need to prove $H_5 \times H_7 \trianglelefteq G$, because:

$H_5 \times H_7 \cong \mathbb{Z}_5 \times \mathbb{Z}_7 \underset{\uparrow \, \gcd(5,7)=1}{\cong} \mathbb{Z}_{35}$, so it is cyclic.

Consider A a conjugate of $H_5 \times H_7$, then $|A| = 35$, so by the 1st Sylow Theorem we have $A_5, A_7 \leq A$ subgroups of A of orders 5 and 7.

Note: $A_5 \leq A \leq G$, $A_7 \leq A \leq G$, so A_5, A_7 are subgroups of G of order 5, 7 respectly.

Since $n_5 = 1 = n_7$, we must have $A_5 = H_5$, $A_7 = H_7$. Now:

$H_5 \leq A$, $H_7 \leq A$, since $H_5 \trianglelefteq G$, $H_7 \trianglelefteq G$ then $H_5 \trianglelefteq A$, $H_7 \trianglelefteq A$, so $H_5 \times H_7 \leq A$, so

by cardinality $H_5 \times H_7 = A$. So $H_5 \times H_7 \trianglelefteq G$.

Alternatively: use elements and that since $H_5, H_7 \trianglelefteq G$ then $H_5 H_7 = H_5 \times H_7$.

Claim: $H_5 H_7 \trianglelefteq G$ by direct computation: let $g \in G$, then:

$$\underset{h \in H_5,\, k \in H_7}{g(hk)g^{-1}} = ghg^{-1}gkg^{-1} = \underset{h' \in H_5,\, k' \in H_7}{h'k'}$$

($H_5 \times H_7 = H_5 H_7$ since $H_5, H_7 \trianglelefteq G$ and $H_5 \cap H_7 = \{e\}$).

(2) - $f: R \to S$ homo. of commutative rings, P prime ideal of S, M maximal ideal of S.

(2) - $f: R \to S$ homo. of commutative rings, P prime ideal of S, M maximal ideal of S.

(a) $f^{-1}(P)$ prime ideal of R.

Pick $a, b \in R$ with $ab \in f^{-1}(P)$, then $f(ab) = f(a)f(b) \in P$, since P prime either $f(a)$ or $f(b) \in P$, then either $a \in f^{-1}(P)$ or $b \in f^{-1}(P)$.

Details: prove/claim $f^{-1}(P)$ is an ideal of R.

(b) If $R \subseteq S$ and f inclusion, use (a) to prove $P \cap R$ is a prime ideal of R.

Notice $f^{-1}(P) = P \cap R$, so it is an ideal. If $p \in P \cap R$ we have $p \in R$ so $f(p) = p$, so $p \in f^{-1}(P)$. If $r \in f^{-1}(P)$ then $r \in R$ and since $r = f(r) \in P$ we have $r \in P$, so $r \in P \cap R$.

(c) If f surjective, then $f^{-1}(M)$ is a maximal ideal of R.

$$\begin{tikzcd} R \arrow[r, two heads, "f"] \arrow[dr, "\phi"'] & S \arrow[d, "\pi"] \arrow[dl, phantom, "\circlearrowright"] \\ & S/M \end{tikzcd}$$

by 1st Iso Theorem:

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d] & S/M \arrow[dl, phantom, "\circlearrowleft"] \\ R/\ker(\phi) \arrow[ur, dashed, "\exists!"'] & \end{tikzcd}$$

$\exists!$ ring hom. $\bar{\phi}$ which is iso since ϕ is surjective because f is. (*)

$$\begin{tikzcd} R \arrow[r, two heads] \arrow[d, "\phi"'] & R/f^{-1}(M) \arrow[dl] \\ S/M & \end{tikzcd}$$

$0 \to f^{-1}(M) \to R \to R/f^{-1}(M) \to 0$

is a short exact sequence.

(*) $R/\ker(\phi) \cong \underbrace{S/M}_{\text{field since } M \text{ maximal}}$, so $\ker(\phi)$ maximal.

Claim: $\ker(\phi) = f^{-1}(M)$ $\quad \phi = \pi \circ f$

$\ker(\phi) = \{r \in R \mid \phi(r) \in M\} = \{r \in R \mid f(r) + M = M\} =$

$= \{r \in R \mid f(r) \in M\} = \{r \in R \mid r \in f^{-1}(M)\} = f^{-1}(M)$.

Alternatively: $f^{-1}(M)$ prime because M max. means M prime, use (a).

Suppose $f^{-1}(M)$ is not maximal, get contradiction using

Suppose $f^{-1}(M)$ is not maximal, get contradiction using $f(R) = S$.

Alternatively: $R/f^{-1}(M) \longrightarrow S/M$ is an isomorphism.

$$(r + f^{-1}(M)) \longmapsto (f(r) + M)$$

③ - R comm. ring, $I \subseteq R$ ideal, $J = \langle I \rangle_{R[x]}$

linear combinations of elements in $R[x]$ with coefficients in I.

(a) $R[x]/J \cong (R/I)[x]$

Idea: construct $\phi : R[x] \longrightarrow (R/I)[x]$, prove $\ker(\phi) = J$, use 1st. Iso Thm.

Alternatively, construct $\psi : R[x]/J \xrightarrow{\cong} (R/I)[x]$, this is very long.

Standard idea

$M \otimes N \xrightarrow{\pi} \frac{M}{I} \otimes \frac{N}{J}$

$\underbrace{I \otimes J}_{\ker(\pi)}$

$\phi : R[x] \longrightarrow (R/I)[x]$, extend by linearity: standard trick

if these are maps, then extension by linearity will be a map

$x \longmapsto x$

$r \longmapsto r + I =: \bar{r}$

$\phi(r_n x^n + \cdots + r_0) := \bar{r}_n x^n + \cdots + \bar{r}_0$

Proving ϕ is map just requires it to be proven on: $\phi(x^k + r) = \phi(x^k) + \phi(r)$. $\phi(x^{m+n}) = \phi(x^m) \cdot \phi(x^n)$.

This is surjective since any $\bar{r}_n x^n + \cdots + \bar{r}_0 = \phi(r_n x^n + \cdots + r_0)$.

Prove $\ker(\phi) = J$: pick $f(x) \in J$, then $f(x) = a_1 f_1(x) + \cdots + a_m f_m(x)$ for some $a_i \in I$, $f_i(x) \in R[x]$.

$f_i(x) = r_{in} x^n + \cdots + r_{i0}$ (we can assume n fixed by setting $r_{jn} = 0$ if necessary).

$\phi(a_i f_i(x)) = \overline{a_i r_{in}}\, x^n + \cdots + \overline{a_i r_{i0}} = 0$, so $f(x) \in \ker(\phi)$.

$a_i \in I$ means $a_i r_{in} \in I$ so $\overline{a_i r_{in}} = 0$.

Let $g(x) \in \ker(\phi)$, so $g(x) = g_n x^n + \cdots + g_0$ with $g_i \in R$; $\phi(g(x)) = 0$ so

$\bar{g}_n x^n + \cdots + \bar{g}_0 = \bar{0}$ so $\bar{g}_i = \bar{0}$ so $g_i \in I$ for all $i = 1, \dots, n$.

comparing coefficients

So $g(x) \in J$.

By the 1st. Iso. Thm.: $\phi(R[x]) = (R/I)[x] \cong R[x]/\ker(\phi) = R[x]/J$.

So $g(x) \in J$. coefficients

By the 1st. Iso. Thm.: $\phi(R[x]) = \left(R/I\right)[x] \cong \dfrac{R[x]}{\ker(\phi)} = \dfrac{R[x]}{J}$.

(b) I prime implies J prime.

R/I is integral domain because I prime.

It is enough to check that $\dfrac{R[x]}{J}$ is integral domain. By (a), it is enough to check $\left(R/I\right)[x]$ is integral domain.

Pick $f(x) = \bar{f}_n x^n + \dots + \bar{f}_0$, $g(x) = \bar{g}_m x^m + \dots + \bar{g}_0$ non-zero elements such that

$\deg(f) = n$ $\qquad$ $\deg(g) = m$ $\qquad$ $\bar{g}_i, \bar{f}_i \in R/I$,

$\bar{f}_n \neq 0$ $\qquad$ $\bar{g}_m \neq 0$ $\qquad$ (So $f(x), g(x) \in \left(R/I\right)[x]$).

and $f(x) \cdot g(x) = 0$. Then: $\deg(f(x) \cdot g(x)) = m+n$ and it has coefficient $\bar{f}_n \cdot \bar{g}_m \neq 0$ because R/I is integral domain. Either contradiction if we assumed $f(x) \cdot g(x) = 0$, or we find $f(x) \cdot g(x) \neq 0$ for all $f(x), g(x)$ non-zero.

④ - $p_1, \dots, p_n$ distinct primes

(a) (i) Show $K_n = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ is Galois over $\mathbb{Q}$.

Note: $\{x^2 - p_1, \dots, x^2 - p_n\}$ has as splitting field K_n, and this is a family of separable polynomials. Hungerford V.3.11. Then K_n is Galois over $\mathbb{Q}$.

(ii) $\operatorname{Gal}(K_n/\mathbb{Q}) \cong \sum_{i=1}^{n} \mathbb{Z}/(2)$.

$\operatorname{Gal}(\mathbb{Q}(\sqrt{p_1})/\mathbb{Q}) \cong \mathbb{Z}/(2)$ because $[\mathbb{Q}(\sqrt{p_1}) : \mathbb{Q}] = 2$, and $\mathbb{Z}/(2)$ is the only group of order 2.

Induction hypothesis: $\operatorname{Gal}(\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n-1}}), \mathbb{Q}) \cong \sum_{i=1}^{n-1} \mathbb{Z}/(2)$.

For n, notice: $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n-1}}) \subsetneq \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ and $x^2 - p_n$ irreducible in this extension. Then this is a degree 2 extension: $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n-1}})(\sqrt{p_n}) \cong \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$.

$n-1$

this extension. Then this is a degree 2 extension: $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_{n-1}})(\sqrt{p_n}) \cong \mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$.

Now: $\underbrace{\sum_{i=1}^{n-1} \mathbb{Z}/(2)}_{\text{just permute } \pm\sqrt{p_i} \leftrightarrow \pm\sqrt{p_i}} \subseteq Gal(K_n/\mathbb{Q})$, and also $[K_n : K_{n-1}] = 2$.

Call $\sigma \in Gal(K_{n-1}/\mathbb{Q})$, then extend it to $\tilde{\sigma} \in Gal(K_n, \mathbb{Q})$ by giving it one of the choices: $\sqrt{p_n} \longmapsto \sqrt{p_n}$.

$\sqrt{p_n} \longmapsto -\sqrt{p_n}$

We then have 2^n total elements in $Gal(K_n, \mathbb{Q})$ so since every element in $Gal(K_n/\mathbb{Q})$ has order 2:

$$Gal(K_n/\mathbb{Q}) \cong \sum_{i=1}^{n} \mathbb{Z}/(2).$$

Alternatively: $\sigma \in Aut(K_n)$, it permutes roots but then $\sqrt{p_i} \longmapsto \pm\sqrt{p_i}$.

Define: $\phi: Aut(K_n) \longrightarrow \sum_{i=1}^{n} \mathbb{Z}/(2)$, this is an iso.

$$\sigma \longmapsto \begin{pmatrix} 0 & \text{if } \sigma(\sqrt{p_j}) = \sqrt{p_j} \\ 1 & \text{if } \sigma(\sqrt{p_j}) = -\sqrt{p_j} \end{pmatrix}_{j=1}^{n}$$

(iii) There are $2^n - 1$ quadratic extensions of $\mathbb{Q}$ contained in K_n. Determine explicitly.

The quadratic extensions of $\mathbb{Q}$ inside $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$ are the splitting fields of $x^2 - \underbrace{p_{i_1}\cdots p_{i_k}}_{\text{pick } k \text{ different primes.}}$ for $i_1,\dots,i_k \in \{1,\dots,n\}$, $i_r \neq i_s$ for all $r,s = 1,\dots,k$.

Such a splitting field is $\mathbb{Q}(\sqrt{p_{i_1}\cdots p_{i_k}})$, and $\mathbb{Q} \underset{\text{degree } 2.}{\subseteq} \mathbb{Q}(\sqrt{p_{i_1}\cdots p_{i_k}}) \subseteq K_n$.

Claim: Since we are adjoining $\sqrt{p_i}$, the only thing we can recover in $\mathbb{Q}$ when taking quadratic powers is $\sqrt{p_{i_1}\cdots p_{i_k}}$.

By the Fundamental Galois Theorem says deg. 2 extensions correspond to subgroups of $\sum_{i=1}^{n} \mathbb{Z}/(2)$ of order 2^{n-1}. There are $2^n - 1$ such subgroups of $\sum_{i=1}^{n} \mathbb{Z}/(2)$ of order 2^{n-1}. There are 2^n-1 such subgroups (that's just the non-empty subsets of $\{1,\dots,n\}$).

For the same reason, $p_{i_1}\cdots p_{i_k}$ corresponds to a non-empty subset of $\{1,\dots,n\}$.

(b) Determine explicitly for $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$: 2, 3, 5, 6, 10, 15, 30.

5 - z generator of $\mathbb{F}_{4^k}$, $k\geq 1$. Prove that $x^{2^k}+x+z^{2^k}+z$ has exactly 2^k roots in $\mathbb{F}_{4^k}$.

$\mathbb{F}_{4^k}$ has characteristic 2. (because it has 4^k elements, which is a power of 2).

$$x^{2^k}+x+z^{2^k}+z = (x^{2^k}+z^{2^k})+(x+z) = (x+z)^{2^k}+(x+z) = (x+z)\left((x+z)^{2^k-1}+1\right).$$

Note $z\in\mathbb{F}_{4^k}$ is a root of $x+z$ (because $\mathbb{F}_{4^k}$ has characteristic 2), and not a root of $(x+z)^{2^k-1}+1$. So we found one root, we only need to prove that $(x+z)^{2^k-1}+1$ factors into 2^k-1 distinct monomials in $\mathbb{F}_{4^k}$.

Recall: We sometimes used that translations preserve the number of roots:

Recurrent trick: $y \longleftrightarrow y+1$; $y-1 \longleftrightarrow y$; $x \longmapsto x+1$

Claim: $y+z$ is a root of $(x+z)^{2^k-1}+1$ iff y is a root of $x^{2^k-1}+1$.

$x \longmapsto x+z$

Then it will be good enough to show that $x^{2^k-1}+1$ splits into 2^k-1 factors in $\mathbb{F}_{4^k}$.

Suppose y is a root of $x^{2^k-1}+1$, then: $((y+z)+z)^{2^k-1}+1 = y^{2^k-1}+1=0$.

Suppose $y+z$ is a root of $(x+z)^{2^k-1}+1$, then:

$y^{2^k-1}+1 = (y+0)^{2^k-1}+1 = ((y+z)+z)^{2^k-1}+1 = 0.$

Recall $\underbrace{\mathbb{F}_{4^k}\text{ is the splitting field of }x^{4^k}+x}_{\text{details}}$, so $\underbrace{x^{4^k-1}+1\text{ has }4^k-1\text{ distinct roots}}_{\text{details}}$.

So if $x^{2^k-1}+1$ divides $x^{4^k-1}+1$, then it has 2^k-1 distinct roots.

Note:

$$x^{4^k-1}+1 = (x^{2^k-1}+1)(x^{4^k-2^k} + x^{4^k-2\cdot 2^k} + \dots + x^{4^k-j\cdot 2^k} + \dots + x^{2^k-1}+1)$$

Trick: Problem 5(b), August 2015: Knowing $d\mid n$: $q^n-1 = (q^d-1)(q^{n-d}+q^{n-2d}+\dots+q^{n-jd}+\dots+q^d+1)$

Trick: Problem 5(b), August 2015: knowing $d|n$: $q^n-1 = (q^d-1)(q^{n-d}+q^{n-2d}+\dots+q^{n-jd}+\dots+q^d+1)$

$$\underbrace{x^{q^n-1}-1 = (x^{q^d-1}-1)(\sim\sim \dots \sim)}_{}$$

in our case $d=2^k$, $n=4^k$, and $+1=-1$ because $\operatorname{char}(\mathbb{F}_{4^k})=2$.

So indeed $x^{2^k-1}+1$ divides $x^{4^k-1}+1$.

(6) - TBD.

(7) - Show that $\mathbb{Q}$ is not a projective $\mathbb{Z}$-mod.

$\mathbb{Z}$ is a P.I.D. Hungerford IV. 6.3. It suffices to show that $\mathbb{Q}$ is not a free $\mathbb{Z}$-mod.

Suppose it is: there is $\phi: \mathbb{Q} \xrightarrow{\cong} \sum_{i\in I} \mathbb{Z}$ iso. of $\mathbb{Z}$-mods, call $e_i := \begin{cases} 0 & j\neq i, \\ 1 & j=i. \end{cases}$

Since ϕ is iso., there is $y \in \mathbb{Q}$ with $\phi(y)=e_i$.

Since $\mathbb{Q}$ is divisible (abelian group), there exists $x\in\mathbb{Q}$ with $2\cdot x = y$. Then:

$2\cdot\phi(x) = \phi(2x) = \phi(y) = e_i$, living in $\sum_{i\in I}\mathbb{Z}$.

However, no element $z \in \sum_{i\in I}\mathbb{Z}$ satisfies $2\cdot z = e_i$, contradiction. So $\mathbb{Q}$ is not free.

Let D an integral domain, Q its field of fractions. Then Q is not projective as D-mod. $(D=\mathbb{Z}, Q=\mathbb{Q})$

Proof: If Q is projective then for some other D-mod R we have:

$R+Q \cong D^n$. This, by restriction, induces a homomorphism from $Q \longrightarrow D^n$, which induces a homomorphism $Q \longrightarrow D$.

However, no such homomorphism $Q \longrightarrow D$ exists. $\square$

$$Q \hookrightarrow R+Q \cong D^n \longrightarrow D$$

(8) - (a) For free group of rank $m\geq 2$, show that a nontrivial normal subgroup cannot be cyclic.

Proof by contrapositive: pick a cyclic subgroup of $F_m = \langle a_1,\dots,a_n\rangle$, we show it is not normal.

Suppose first the cyclic subgroup is $\langle a_i\rangle$. Since $m\geq 2$, there is $a_j\neq a_i$ where $a_ja_ia_j^{-1}$ is a reduced word. However, all reduced words in $\langle a_i\rangle$ are of the form a_i^n, $n\in\mathbb{Z}\setminus\{0\}$, a reduced word. However, all reduced words in $\langle a_i \rangle$ are of the form a_i^n, $n \in \mathbb{Z} \setminus \{0\}$,

so $a_j a_i a_j^{-1} \notin \langle a_i \rangle$, so $\langle a_i \rangle \ntrianglelefteq F_m$.

Suppose we have $\langle g \rangle$ for some general $g \in F_m$: $g = a_{i_1}^{r_1} a_{i_2}^{r_2} \cdots a_{i_k}^{r_k}$, where $r_j \in \mathbb{Z} \setminus \{0\}$

and $i_j \neq i_{j+1}$ for $j = 1, \dots, k-1$.

$\underline{m=3}$: pick $a_{i_1} \neq a_j \neq a_{i_k}$. Then $\langle g, a_j \rangle$ is a free group on more than one generator containing the cyclic subgroup $\langle g \rangle$, so by the above, $\langle g \rangle \ntrianglelefteq \langle g, a_j \rangle$ so $\langle g \rangle \ntrianglelefteq F_m$.

$\underline{m=2}$: If $a_{i_1} = a_{i_k} =: a_1$, then $\langle g, a_2 \rangle$ is a free group on two generators, so as above $\langle g \rangle \ntrianglelefteq F_m$.

If $a_{i_1} \neq a_{i_k}$, rename $a_{i_1} =: a_1$ if $r_1 > 0$, $a_{i_1} =: a_1^{-1}$ if $r_1 < 0$; similarly relabel $a_{i_k} =: a_2, a_2^{-1}$. Then:

$$g^n = \underbrace{\underbrace{a_1^{r_1} a_2^{r_2} \cdots a_1^{r_{k-1}} a_2^{r_k}}_{1} \underbrace{a_1^{r_1} a_2^{r_2} \cdots a_1^{r_{k-1}} a_2^{r_k}}_{2} \cdots \underbrace{a_1^{r_1} a_2^{r_2} \cdots a_1^{r_{k-1}} a_2^{r_k}}_{n}}_{n}$$

$$g^{-n} = a_2^{-r_k} a_1^{-r_{k-1}} \cdots a_2^{-r_2} a_1^{-r_1} \cdots a_2^{-r_k} a_1^{-r_{k-1}} \cdots a_2^{-r_2} a_1^{-r_1}$$

$a_1 g a_1^{-1} = a_1^{r_1+1} a_2^{r_2} \cdots a_1^{r_{k-1}} a_2^{r_k} a_1^{-1}$ is $\underline{\text{not}}$ $g^{\pm n}$ for any $n \in \mathbb{Z} \setminus \{0\}$, but it is $\underline{\text{not}}$ trivial. So $a_1 g a_1^{-1} \notin \langle g \rangle$, so $\langle g \rangle \ntrianglelefteq F_2$.

(b) Show that a solvable group cannot contain F_2 as a subgroup.

We will use that subgroups of free groups are free (hint), and that subgroups of solvable groups are also solvable. Hungerford II.7.11. So it is enough to prove that F_2 is $\underline{\text{not}}$ solvable.

if they have a non-finite number of generators, everything still follows.

Def: A group G is $\underline{\text{solvable}}$ if its derived series:

$G \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \dots$ eventually has $\{e\}$ in it.

$G^{(i+1)} := [G^{(i)}, G^{(i)}]$.

A group G is $\underline{\text{solvable}}$ if it has a subnormal series whose quotient groups are abelian:

$\{e\} = G_0 < G_1 < \dots < G_k = G$ with $G_{j-1} \trianglelefteq G_j$ and G_j / G_{j-1} is abelian $j = 1, \dots, k$.

$\{e\} = G_0 < G_1 < \cdots < G_k = G$ with $G_{j-1} \triangleleft G_j$, $j=1,\dots,k$ and G_j / G_{j-1} is abelian $j=1,\dots,k$.

Consider $[F_2,F_2] < F_2$, it is a normal subgroup. Since it is a subgroup of a free group, it must also be free. Since F_2 is not abelian, $[F_2,F_2] \neq \{e\}$, and since $[F_2,F_2] \triangleleft F_2$ by part (a) it is not cyclic, so $[F_2,F_2] \ncong F_1$. So $[F_2,F_2] \cong F_{m_1}$ for $m_1 \geq 2$.

Inductively, if F_{m_k} a free group on $m_k \geq 2$ generators, then $[F_{m_k}, F_{m_k}] \triangleleft F_{m_k}$ that is also a free group. By (a), it cannot be cyclic, then $[F_{m_k}, F_{m_k}] \cong F_{m_{k+1}}$.

Now:

$$\underset{\cong F_2}{F_2} \rhd \underset{F_{m_1}}{\underset{\cong}{F^{(1)}}} \rhd \underset{F_{m_2}}{\underset{\cong}{F^{(2)}}} \rhd \cdots \rhd \underset{F_{m_i}}{\underset{\cong}{F^{(i)}}} \rhd \cdots$$

where $F^{(i)} \cong F_{m_i} \neq \{e\}$, so the derived series will never have $\{e\}$.

⑨ - $f(x) = x^5 + x + 1$

(a) Find $[K:\mathbb{Q}]$, K splitting field of $f(x)$ over $\mathbb{Q}$.

$$x^5+x+1 = \underbrace{(x^2+x+1)}_{\text{both}}\underbrace{(x^3-x^2+1)}_{\text{irreducible}}, \text{ so } [K:\mathbb{Q}] \underset{\uparrow \circledast}{=} [K:K_3][K_3:\mathbb{Q}] = 2\cdot 6 = 12$$

roots $\omega, \bar{\omega}$ roots $r, \alpha, \bar{\alpha}$

splitting field of x^3-x^2+1: $K_3 = \mathbb{Q}(r,\alpha)$, and now: $[\mathbb{Q}(\alpha,r):\mathbb{Q}] = 6$.

splitting field of x^2+x+1: $K_2 = \mathbb{Q}(r,\alpha)(\omega) = \mathbb{Q}(r,\alpha,\omega)$ (over K_3)

this is also: $K = K_2 = \mathbb{Q}(r,\alpha,\omega)$. ⊛

(b) $\mathrm{Aut}_{\mathbb{Q}}(K)$ of $f(x)$.

Notice: $\mathrm{Gal}(\mathbb{Q}(\alpha,r)/\mathbb{Q}) = S_3$

Hungerford V.4.7.

Hungerford V.4.7.

The discriminant of $x^3 - x^2 + 1$ is -23, which is never a square in $\mathbb{Q}$.

Then by the Extension of Isomorphism Theorem:

$$Gal(K/\mathbb{Q}) = \mathbb{Z}/(2) \times S_3.$$