① Either prove true/false:

ⓐ If $H, K \leq G$ then either HK or KH is a subgroup.

↳ False: In $GL_2(\mathbb{Z}_2)$, $UT_2 LT_2$ and $LT_2 UT_2$ are not subgps as

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

and ↑ is not in $GL_2(\mathbb{Z}_2)$.

ⓑ Every finite gp G is isomorphic to a subgp of $GL_n(\mathbb{C})$ for some n.

↳ True: By Cayley's theorem, $G \cong$ a subgp of S_n for some n, and there is an isomorphic copy of S_n in $GL_n(\mathbb{C})$ consisting of the permutation matrices.

②

2) Let $G = H \ltimes U$ be a finite group, for groups H and U. Let p be prime, and let $\mathrm{Syl}_p(G)$ denote the set of Sylow p-subgroups of G.

(a) Show that if $\mathrm{Syl}_p(G) \cap \mathrm{Syl}_p(U) \neq \emptyset$, then $\mathrm{Syl}_p(G) = \mathrm{Syl}_p(U)$.

(b) Suppose $\mathrm{Syl}_p(G) \cap \mathrm{Syl}_p(U) \neq \emptyset$ and $\gcd(|H|, |U|) = 1$. Prove that H acts transitively on $\mathrm{Syl}_p(U)$ if and only if $Q \trianglelefteq U$ for some $Q \in \mathrm{Syl}_p(G)$.

ⓐ All of the Sylow p-subgps of G are conjugate to one another. If some $P \in Syl_p(G)$ is also a Sylow p-subgp of U, then $|G| = p^k n$ and $|U| = p^k m$ for $p \nmid m, n$.
Now, note that as $G = H \ltimes U$, $U \trianglelefteq G$, and thus $gPg^{-1} \subseteq U$ for all $g \in G$.
If G had a Sylow subgroup not in U, then P could not be conjugate to that subgroup, violating Sylow's theorem.

ⓑ Suppose first that $Q \trianglelefteq U$ for some $Q \in Syl_p(G)$. Note that as $Syl_p(G) = Syl_p(U)$, and all Sylow p-subgroups of U are conjugate in U, this implies that Q is the unique Sylow p-subgroup of U and thus it is trivial that H acts transitively on $Syl_p(U)$.
Conversely, say H acts transitively on $Syl_p(U)$ and let $Q \in Syl_p(U)$.
Then $|H(Q)| = \frac{|Syl_p(U)|}{|Stab_H(Q)|}$. Since $|Syl_p(U)|$ divides $|U|$, and $|Stab_H(Q)| \,\big|\, |H|$ with $\gcd(|U|, |H|) = 1$, we must have $|Stab_H(Q)| = 1$, so that H acts transitively on $Syl_p(U)$. ∎

3) Let R be the subring of $\mathbb{Q}$ consisting of fractions with odd denominators in reduced form; you may assume without proof that R is a ring.

(a) Prove that all irreducible elements of R, and all prime elements of R, are of the form $2u$ for some invertible element u of R.

(b) Prove that R is Euclidean. [Hint: consider the function $v : R\backslash\{0\} \to \mathbb{Z}$ for which $v(2^k u) = k$ whenever u is a unit.]

ⓐ Let $r \in R$ be irreducible. Note the units of r are the odd integers, and the fractions w/ odd numerators + denominators. ($\mathbb{Q}$ is an integral domain, and thus R is, so showing this for irreducibles takes care of primes too).

$r = ab$ and one of a, b is a unit.

claim $ab = 2u$ for u a unit.

Note 2 is not a unit as $\frac{1}{2} \notin R$
anything w/ more than 1 power of 2 in the numerator is not irreducible as $2 \cdot \frac{2}{u}$ is a product of two non-units. If r has no power of 2 in the numerator, then r is not irreducible since it is a unit.

ⓑ Let $a, b \in R$. If b is a unit, then
$a = (ab^{-1})b$ and we are done.

Otherwise, $b = 2^k u$ for $u \in R^\times$ and $k \geq 1$.

Then $a = (2^k u)u^{-1}a$ -

$a = 2^\ell v$, suppose $\ell \geq k$.

$$2^\ell v = (2^k u)(2^{\ell-k} u^{-1} v)$$

If $\ell < k$,

$$2^\ell v = (2^k u)(\quad) - (\quad)$$
$$= 2^\ell(2^{k-\ell}(\quad) - (\quad)).$$

(as v a unit, its numerator is not divisible by 2 so $\exists$ a way to write $v = 2^{k-\ell}(\quad) \pm (\quad)$

divisible by not 2.

(4) Done already, see Canonical_forms.xopp.

5) Let p be a prime number, $\mathbb{F}_p$ be the field with p elements, and $F = \mathbb{F}_p(t)$, where t is an indeterminate.

(a) Prove that the polynomial $x^p - t$ is irreducible over F. [Hint: consider factorizations over the polynomial ring $\mathbb{F}_p[t]$ and use Gauss's Lemma.]

(b) Let α be a root of $x^p - t$, and let $E = F(\alpha)$. Find the degree of E over F, and find the automorphism group $\mathrm{Aut}(E/F)$.

(a) If $x^p - t$ is irreducible over $\mathbb{F}_p[t]$, it is irreducible over $\mathbb{F}_p(t)$ by Gauss' lemma, as $\mathbb{F}_p[t]$ is a UFD.

- Eisenstein's lemma: the constant term belongs to (t) but not $(t)^2 = (t^2)$

so by Eisenstein, $x^p - t$ is irreducible over $\mathbb{F}_p[t]$.

(b) Since α a root of $x^p - t$, and this polynomial is irreducible over F,

$$[E:F] = \deg(m_\alpha(x)) = p.$$

Since $\mathbb{F}_p$ has p elements, $|\mathbb{F}_p^\times| = p-1$ so $x^p = x \ \forall x \in \mathbb{F}_p$.

$\alpha = \sqrt[p]{t}$ and $(x - \sqrt[p]{t})^p = x^p - t$, so α is the only root of $x^p - t$.

Thus, $\mathrm{Aut}(E/F)$ is trivial.

still true if $p=2$ as $t = -t$ in $\mathbb{F}_2$.

6) Suppose F is a field, K is the splitting field of a degree 4 separable polynomial in $F[x]$, and $[K : F] = 8$.

(a) Find $\mathrm{Gal}(K/F)$, up to isomorphism.

(b) How many degree two subextensions are there of K/F?

K is an 8-dimensional vector space over F, and $|\mathrm{Gal}(K/F)| = 8$.

Thus $\mathrm{Gal}(K/F)$ is either D_8 or a subgroup of S_4 or A_4.

- A_4 has no subgp of order 8.
- S_4 has only D_8 as an order 8 subgroup,

so $\mathrm{Gal}(K/F) \cong D_8$.

(b) A deg 2 subextension $F \subseteq E \subseteq K$ corresponds to an index 2 subgp of D_8, of which there is exactly 1.