Practice Exam Suggested Solutions.

Problem 1 G cyclic of order 12

then $G \cong \mathbb{Z}_{12} = \langle 1 \rangle$. The subgroups

correspond to divisors of 12 which

are: 1, 2, 3, 4, 6, 12.

Therefore the subgroups are:

$\langle 1 \rangle = G$ order 12

$\langle 2 \rangle$ order 6

$\langle 3 \rangle$ order 4

$\langle 4 \rangle$ order 3

$\langle 6 \rangle$ order 2

$\{0\}$

2. $H = \langle (1,2,3,4) \rangle \leq S_4$ (question should have specified left or right cosets)

$(1,2,3,4)$ has order 4 in S_4.
So H has size 4.

Therefore the # of left cosets is

$$[S_4 : H] = \frac{|S_4|}{|H|} = \frac{24}{4} = 6.$$

H itself is a coset. It's elements are:

$$H = \{e, (1,2,3,4), (1,3)(2,4), (1,4,3,2)\}.$$

Since $(1,3)$ is not in H, another left coset is

$$(1,3)H = \{(1,3), (1,2)(3,4), (24), (1,4)(2,3)\}.$$

3. Let p be prime and N a normal p-subgroup of a finite group G.

First by Sylow's 1st theorem N is contained in a Sylow p-subgroup P_0.

Now consider an arbitrary p-Sylow subgroup P. By Sylow's 2nd theorem $\exists\ g \in G$ s.t.

$$P = g^{-1} P_0 g = \{g^{-1} h g \mid h \in P_0\}$$

Now suppose $n \in N$, then since N is normal $\exists\ g \in G$ and $n' \in N \leq P_0$ s.t.

$n = g^{-1} n' g$. Therefore, $n \in P$ hence $N \leq P$ for every p-Sylow subgroup P $\square$.

Problem 2

$f(x) = x^2 - 1 = (x+1)(x-1) \in \mathbb{Q}[x]$.

Hence $\langle f(x) \rangle$ is not a prime ideal and $R = \mathbb{Q}[x]/\langle x^2 - 1 \rangle$ is not an integral domain.

Alternatively: notice $(x+1)(x-1) = 0$ in R however $x+1, x-1 \neq 0$ in R.

Every field is also an integral domain hence R is <u>not</u> a field.

2. R, S commutative rings with unity.

$\Phi : R \to S$ a surjective ring homom.

Let $M \subseteq S$ be a maximal ideal

consider $\Phi^{-1}(M) = \{a \in R \text{ s.t. } \Phi(a) \in M\}$

Aside:

Note $\Phi^{-1}(M)$ is an ideal in R

since the preimage of an additive subgroup under a homomorphism is an additive subgroup and for any $r \in R$

if $a \in \Phi^{-1}(M)$ then $\Phi(ra) = s \cdot \Phi(a)$

$= s \cdot m \in M$ so $ra \in \Phi^{-1}(M)$.

Now suppose $\Phi^{-1}(M)$ is not maximal. Then there is a proper ideal $\tilde{M}$ of R such that $\Phi^{-1}(M) \subsetneq \tilde{M}$.

Then $M \subseteq \Phi(\tilde{M})$. Since M is maximal in S, there are two possibilities: either $M = \Phi(\tilde{M})$ (case 1) or $\Phi(\tilde{M}) = S$. (case 2)

If $M = \Phi(\tilde{M})$, then

$$\tilde{M} \overset{\circledast}{\subseteq} \Phi^{-1}\Phi(\tilde{M}) = \Phi^{-1}(M).$$

where the inclusion $\circledast$ holds since the preimage of $\Phi(\tilde{M})$ must at least contain $\tilde{M}$. But by assumption $\Phi^{-1}(M) \subseteq \tilde{M}$. Hence $\tilde{M} = \Phi^{-1}(M)$.

If $\Phi(\tilde{M}) = S$ then for every $r \in R$ there exists an $m \in \tilde{M}$ s.t.

$$\Phi(r) = \Phi(m) \Rightarrow \Phi(r-m) = 0$$

since $0 \in M$, $r - m \in \Phi^{-1}(M) \subseteq \tilde{M}$

Since $m \in \tilde{M}$ and $\tilde{M}$ is an ideal, we have $r \in \tilde{M}$ for every $r \in R$.

$$\Rightarrow \tilde{M} = R$$

Combining the two cases implies that $\tilde{M} = R$ or $\tilde{M} = \Phi^{-1}(M)$.

Hence $\Phi^{-1}(M)$ is maximal in R.

<u>Example</u> Consider the homomorphism $f : \mathbb{Z} \to \mathbb{Z}_3$ and the maximal ideal $I = \langle 2 \rangle \subseteq \mathbb{Z}$.

Then $f(\langle 2 \rangle) = \{0, 1, 2\} = \mathbb{Z}_3$.

So $f(I)$ is not a maximal ideal of $\mathbb{Z}_3$.

3. let J_1, J_2 be ideals of R.

Define $J_1 + J_2 = \{a_1 + a_2 \in R \mid a_1 \in J_1, a_2 \in J_2\}$

Firstly $J_1 + J_2$ is an additive subgp of R.

<u>Closed</u> If $a, b \in J_1 + J_2$ then

$a = a_1 + a_2 \quad a_i \in J_i$

$b = b_1 + b_2 \quad b_i \in J_i$

So $a + b = a_1 + a_2 + b_1 + b_2$

$$= (a_1 + b_1) + (a_2 + b_2)$$

$$= a_1' + a_2' \in J_1 + J_2$$

$\Rightarrow J_1 + J_2$ is closed under addition

<u>Identity</u> $0 = 0 + 0 \in J_1 + J_2$

<u>Inverses</u> $a = a_1 + a_2 \in J_1 + J_2 \quad -a = -a_1 - a_2$

where $-a_i \in J_i$ hence $-a \in J_1 + J_2$.

Now given $a = a_1 + a_2 \in J_1 + J_2$

$ra = r(a_1 + a_2) = ra_1 + ra_2$

$ra_i \in J_i$ since J_i is an ideal

$\Rightarrow \quad ra \in J_1 + J_2$.

$J_1 + J_2$ is an ideal.

$\ker \Phi = \{ a \in R : \Phi(a) = 0 \in R/J_1 \times R/J_2 \}$.

$$\left\{ a \in R \;\middle|\; \begin{array}{l} a + J_1 = J_1 \text{ and} \\ a + J_2 = J_2 \end{array} \right\}$$

$a + J_i = J_i \iff a \in J_i$. Therefore

$\ker \Phi = \{ a \in R \mid a \in J_1, a \in J_2 \}$

$= J_1 \cap J_2$.

Problem 3 $F = \mathbb{Z}_5$

1) Show $f(x) = x^3 + x + 1 \in F[x]$ is irreducible over F.

$\deg f(x) = 3$ so if it is reducible over F it must have a linear factor.

Check: $f(0) = 1 \neq 0$
$f(1) = 3 \neq 0$
$f(2) = 1 \neq 0$
$f(3) = 1 \neq 0$
$f(4) = 4 \neq 0$

Hence the polynomial is irreducible over F.

2. Explain why $f(x)$ divides $x^{5^3} - x$ over F.

Let α_1 be a zero of $f(x)$ in $\overline{F}$.

Since $f(x)$ is irreducible and of degree 3, $F(\alpha_1)$ is a field of size 5^3. In ~~fact~~

$$F(\alpha_1) = \{\alpha \in \overline{F} \mid \alpha^{5^3} - x\}.$$

Since F is finite $f(x)$ splits over the field $F(\alpha_1)$ as

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

for $\alpha_1, \alpha_2, \alpha_3 \in F(\alpha_1)$. Therefore

$$\alpha_i^{5^3} - \alpha = 0 \quad \text{and the}$$

zeros of $f(x)$ are zeros of $x^{5^3} - x$; and we have that $f(x)$ divides $x^{5^3} - x$.

Applying the division algorithm we find an $g(x) \in F[x]$ s.t.

$$x^{5^3} - x = f(x) g(x).$$

3. Let $\alpha \in \overline{F}$ be a zero of $f(x)$

A basis for $E = F(\alpha)$ over F

is $\{1, \alpha, \alpha^2\}$ since $\deg f = 3$.

The Frobenius automorphism in this case is:

$$\sigma : F(\alpha) \to F(\alpha)$$
$$a \mapsto a^5$$

The Galois group is:

$G(E/F) = \langle \sigma \rangle$ so powers of σ send α to other zeros of $f(x)$

The roots are α, $\sigma(\alpha)$, $\sigma^2(\alpha)$

$$\sigma(\alpha) = \alpha^5, \quad \sigma^2(\alpha) = (\alpha^5)^5$$

$$\sigma(\alpha) = \alpha^5 = \alpha^2\alpha^3 = \alpha^2(-\alpha-1)$$

$$= -\alpha^3 - \alpha^2$$

$$= -(-\alpha-1) - \alpha^2$$

$$= 4\alpha^2 + \alpha + 1$$

$$\sigma^2(\alpha) = (\sigma^5)^5 = (4\alpha^2+\alpha+1)^5 \quad \text{(Freshman's dream)}$$

$$= (4\alpha^2)^5 + \underbrace{\alpha^5}_{\text{calculated above}} + 1$$

$$= 4\alpha^{10} + 4\alpha^2 + \alpha + 2$$

see next page

$$= 4(3\alpha^2 + 3\alpha + 3) + 4\alpha^2 + \alpha + 2$$

$$= 2\alpha^2 + 2\alpha + 2 + 4\alpha^2 + \alpha + 2$$

$$= \alpha^2 + 3\alpha + 4$$

$$\alpha^{10} = (\alpha^5)^2 = (4\alpha^2 + \alpha + 1)^2 =$$

$$= \alpha^4 + \alpha^2 + 1 + 8\alpha^3 + 8\alpha^2 + \alpha$$

$$= \alpha(\alpha^3) + 3\alpha^3 + 4\alpha^2 + \alpha + 1$$

$$= \alpha(-\alpha-1) + 3(-\alpha-1) + 4\alpha^2 + \alpha + 1$$

$$= 4\alpha^2 + 4\alpha + 2\alpha + 2 + 4\alpha^2 + \alpha + 1$$

$$= 3\alpha^2 + 3\alpha + 3.$$

Alternative to solving $\sigma^2(\alpha)$ could notice:

we know $\sigma^2(\alpha) = a\alpha^2 + b\alpha + c$ a, b, c GF.

$$f(x) = x^3 + 0 \cdot x^2 + x + 1 = (x-\alpha)(x-\sigma(\alpha))(x-\sigma^2(\alpha))$$

$$= x^3 - \underbrace{(\alpha + \sigma(\alpha) + \sigma^2(\alpha))}_{=0} x^2 + \text{------}$$ multiplying out

So $\alpha + 4\alpha^2 + \alpha + 1 + a\alpha^2 + b\alpha + c = 0 \implies$
$a = 1,\ b = 3,\ c = 4.$ $\square$

Problem 4. $p > 2$ prime # $f(x) \in \mathbb{Q}[x]$ irred. of degree p. K is splitting field of f.

1) $\alpha \in \overline{\mathbb{Q}}$ a zero of f then

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg \operatorname{irr}(\alpha, \mathbb{Q}) = \deg f(x) = p.$$

2) Let $\alpha_1, \ldots, \alpha_p$ be the distinct roots of $f(x)$. (They are distinct since $f(x)$ is irreducible and $\mathbb{Q}$ is perfect).

$\sigma \in G(K/\mathbb{Q})$ permutes α_i's

hence we view $G(K/\mathbb{Q}) \leq S_p$.

$[K:\mathbb{Q}] = |G(K/\mathbb{Q})|$ moreover

$$[K:\mathbb{Q}] = [K:\mathbb{Q}(\alpha_i)][\mathbb{Q}(\alpha_i):\mathbb{Q}].$$

$$= [K:\mathbb{Q}(\alpha_i)] \cdot p.$$

so p divides $|G(K/\mathbb{Q})|$ hence by Sylows theorem there is a subgroup of order p $H \leq G(K/\mathbb{Q})$

Moreover H must be cyclic so $H = \langle \sigma \rangle$ with σ a permutation of order p. The only permutations of order p in S_p are cycles of length p.

Hence $G(K/\mathbb{Q})$ contains a cycle of length p.

Suppose f has $p-2$ zeros which are $\mathbb{Q}$-conjugate.

Let $\tau : \mathbb{C} \to \mathbb{C}$ denote the field automorphism of $\mathbb{C}$-conj.

We can restrict τ to K to obtain an isomorphism:

$\tau : K \to K' \leq \bar{\mathbb{Q}}$. Moreover $K = K'$ since $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_p)$ and $\tau(\alpha_1) = \alpha_2$ if α_1, α_2 are the complex conjugate roots. and $\tau(\alpha_i) = \alpha_i$ $i \neq 1, 2$.

So $\tau \in G(K/\mathbb{Q})$ and τ is the transposition $(1,2)$ if α_1, α_2 are the $\mathbb{C}$-conjugated roots

3. Conclude $G(K/\mathbb{Q}) \cong S_p$.
For which p is $G(K/\mathbb{Q})$ solvable?

We claim S_n is generated by an n-cycle and a single transposition [say $(1,2)$] for any n.
Recall: every permutation in S_n can be written as a product of transpositions. Therefore if we can write every transposition in terms of the n-cycle and $(1,2)$ we are done.
Without loss of generality we can assume that the n-cycle is $(1, 2, 3, \ldots, n)$.

Then computing we get

$$\sigma^k \tau \sigma^{-k} = (k+1, k+2)$$

for $k = 0, \ldots, n-2$.

Therefore we can obtain the transpositions of the form

$$(1,2), (2,3), \ldots, (n, n-1).$$

For $i<j$ we have

$$(i,j) = (j-1,j) \cdots (i+1,i+2)(i,i+1)(i+1,i+2) \cdots (j-1,j).$$

Therefore every permutation in S_p can be expressed as a product of the cycle of length p and the transposition arising from $\mathbb{C}$-conjugation $\Rightarrow G(K/\mathbb{Q}) \cong S_p$.

S_n is not solvable for $n \geq 5 \Rightarrow$ f is solvable for $p = 2, 3$. $\square$