1. Prove that, up to isomorphism, there is a unique group of order 1001 ($= 7 \times 11 \times 13$).

Proof: Suffices to show all the Sylow p-subgroups are unique.

$n_7 \mid 11 \cdot 13$ and is $\equiv 1 \bmod 7$. So can't be 11, or 13.

$11 \cdot 13 = 143 \equiv 3 \bmod 7$

so $n_7 = 1$.

$n_{11} \mid 7 \cdot 13$, $n_{11} \equiv 1 \bmod 11$. Can't be 7 or 13.

$7 \cdot 13 = 70 + 21 = 91 \equiv 3 \bmod 11$.

so $n_{11} = 1$

$n_{13} \mid 7 \cdot 11$ and is $\equiv 1 \bmod 13$.

$7 \cdot 11 = 77 \equiv 12 \bmod 13$ so $n_{13} = 1$.

Thus $G = \mathbb{Z}_7 \times \mathbb{Z}_{11} \times \mathbb{Z}_{13}$.

2. Let S_n be the symmetric group on n symbols.

(i) Prove that if $2 \leq n \leq 4$ then there is a surjective homomorphism of groups from S_n to S_{n-1}.

(ii) Prove that if $n \geq 5$ then there is no surjective homomorphism of groups from S_n to S_{n-1}.

(i) $S_2 \to S_1$ this is trivial.

$S_3 \to S_2$ the sign homomorphism (can't just ignore the cycle containing n).

odd $\mapsto (12)$, even $\mapsto id$.

$S_4 \to S_3$ need a normal subgp of order 4: S_4 has one subgp of order 8, D_8, by Sylow.

The subgroup R of rotations in D_8 is the only order 4 subgp of D_8, so as conjugation by $g \in S_4$ is an automorphism of D_8, we have that $R \trianglelefteq S_4$, and since $[S_4, S_4] \nsubseteq R$, S_4/R is nonabelian of order 6, so is $\cong S_3$.

(ii) If $\exists$ surjective $\varphi: S_n \to S_{n-1}$, then $S_n/\ker\varphi \cong S_{n-1}$

and thus $|\ker\varphi| = n$. Why can't this happen for $n \geq 5$?

Does S_5 have a unique 5-subgroup?

$(1\ 2\ 3\ 4\ 5)$, $(1\ 3\ 5\ 2\ 4)$, $(1\ 4\ 2\ 5\ 3)$, $(1\ 5\ 4\ 3\ 2)$

No! Several subgps of order 5, each conjugate to each other, so $\nexists$ surjective hom to S_4.

- WTS S_n has no normal subgp of order n for $n \geq 5$.

- A_n is only normal subgroup:

Let $N \trianglelefteq G$. Since A_n simple, and $N \cap A_n \trianglelefteq A_n$ (as $A_n \trianglelefteq S_n$)

we have that $N \cap A_n = \{1\}$ or A_n. If $N \cap A_n = \{1\}$, then since A_n is the commutator subgroup of S_n, $N \subseteq Z(S_n) = \{1\}$ and N is trivial.

Else, since $[S_n : A_n] = 2$, N cannot properly contain A_n. So S_n has no homomorphism onto S_{n-1} as it cannot have a hom. w/ kernel of order n since kernels are $\trianglelefteq$.

3. Let R be a commutative ring with identity.

(i) Suppose that I is an ideal of R that is contained in the principal ideal $\langle a \rangle$. Show that there is an ideal J of R such that $I = \langle a \rangle J$.

(ii) Now suppose that $R = \mathbb{C}[x, y]$. Give an example of two ideals $I \subseteq A$ of R for which there is no ideal J satisfying $I = AJ$.

(i) Consider the ideal ${}_aR = \{r \in R \mid ar \in I\}$.

This is an ideal as if $r, s \in {}_aR$,

$a(r+s) = ar + as \in I$

and if $r \in {}_aR$, $s \in R$,

$rs \in {}_aR$ since $a(rs) = (ar)s \in I$.

$\langle a \rangle J \subseteq I$: If $x \in \langle a \rangle J$, $x = (ra)s = r(\underset{I}{\underset{\cap}{as}}) \in I$.

$I \subseteq \langle a \rangle J$: $I \subseteq \langle a \rangle$ so every

$x \in I$ is $x = ra$ for some $r \in R$

$x = ar$ and since $x \in I$, $r \in {}_aR$.

(ii) By part 1, A cannot be a principal ideal.

Let $A = (x, y)$

and $I = (x^2)$. Note if J is s.t. $I \subseteq AJ$ then

J must contain the element x; but then $xy \in AJ$, and $xy \notin I$.

4. Let F be a field and let $A \in M_n(F)$ be a non-invertible $n \times n$ matrix over F.

(i) Prove that if 0 is the only eigenvalue of A in F, and F is algebraically closed, then we have $A^n = 0$.

(ii) Find an example of a field F and a non-invertible matrix $A \in M_n(F)$ such that 0 is the only eigenvalue of A in F, but such that we do not have $A^n = 0$.

(i) If 0 is the only eigenvalue of A, then the JCF of A is strictly upper triangular, and all strictly upper triangular matrices are nilpotent and

$$A = BJB^{-1} \Rightarrow A^n = BJ^nB^{-1} = B \cdot 0 \cdot B^{-1} = 0.$$

(ii) F cannot be algebraically closed. Want a matrix with eigenvalues $0, \sqrt{2}$ over $\mathbb{Q}$.

want Matrix w/characteristic polynomial

$$x(x^2-2) = x^3 - 2x$$

$$\begin{vmatrix} x & 0 & 0 \\ 0 & x & 2 \\ 1 & 1 & x \end{vmatrix} = x^3 - 2x$$

so
$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -2 \\ -1 & -1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 0 & 0 & 0 \\ 2 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -2 \\ -1 & -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -4 \\ -2 & -2 & 0 \end{bmatrix} \neq 0.$$

look up how we know the codomain is K ⇝ $N(\alpha)$ is the product of the Galois conjugates of α, which is the constant term (up to mult. by -1) of $m_\alpha(x)$ over K

5. Let L/K be a Galois extension of fields. The *norm* map from L to K is defined to be

$$N(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

(i) Show that N restricts to a homomorphism of groups from L^* to K^*.

(ii) Let $\mathbb{F}_q$ denote the field with q elements and let m be a positive integer. Show that $N : \mathbb{F}_{q^m}^* \to \mathbb{F}_q^*$ is surjective. [Hint: use the Frobenius automorphism.] true if q not prime?

(iii) Let σ be a generator for $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Compute the cardinality of

$$S = \left\{ \frac{\alpha}{\sigma(\alpha)} \;\middle|\; \alpha \in \mathbb{F}_{q^m}^* \right\}.$$ all of $\mathbb{F}_q^\times$ goes to 1 as $\sigma(\alpha) = \alpha$

(iv) Show that $\ker(N) = S$, where N and S are as defined in parts (ii) and (iii) respectively.

(i) Let $\alpha, \beta \in L^*$. Then

$$N(\alpha\beta) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha\beta) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha)\sigma(\beta) = \left(\prod_{\sigma\in G} \sigma(a)\right)\left(\prod_{\sigma \in G}\sigma(b)\right) = N(\alpha)N(\beta).$$

Since only $N(0)=0$, we have $N(\alpha\beta) \in K^*$.

(ii) If $q = p^n$, then the Galois group of $\mathbb{F}_{q^m}^\times$ over $\mathbb{F}_p$ is cyclic of order mn, generated by the Frobenius Automorphism $\sigma_p : x \mapsto x^p$. Now,

$\mathbb{F}_q$ has Galois group over $\mathbb{F}_p$ of order n generated by σ_p.

As $\mathbb{F}_q$ is the fixed field of $\langle \sigma_p^n \rangle$, we have $H := \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle \sigma_p^n \rangle$ has order m.

the relevant part.

Moreover, $K = \mathbb{F}_{q^m}$ is a finite, separable extension of $F = \mathbb{F}_q$, so $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$ for some α.

Also, α generates $\mathbb{F}_{q^m}^\times$ so that $|\alpha| = q^m - 1$

and
$$N(\alpha) = \alpha \cdot \sigma_p^n(\alpha) \cdot \sigma_p^{2n}(\alpha) \cdots \sigma_p^{(m-1)n}(\alpha) = \alpha^{1+q+\dots+q^{m-1}}.$$

Then the order of this element is $q-1$ since $q^m - 1 = (q-1)(1+q+\dots+q^{m-1})$.

Thus $N(\alpha)$ generates $\mathbb{F}_q^\times$.

(iii) Going by info in part (iv), if $\ker(N) = S$ and N is a surjective hom from $\mathbb{F}_{q^m}^\times \to \mathbb{F}_q^\times$, by 1st Isom. we know $|S|$ should be $1 + q + \dots + q^{m-1}$.

order $q^m - 1$ ↓ ↙ $q-1$

The 1 comes from all of $\mathbb{F}_q$ collapsing to the identity when dividing $\frac{a}{\sigma(a)}$

Recall α generates $\mathbb{F}_{q^m}^\times$, so — Showing (iv) gives (iii)

(iv) Easy to show $S \subseteq \ker(N)$:

$$N\left(\frac{a}{\sigma(a)}\right) = \frac{a \cdot \sigma(a) \cdot \sigma^2(a) \cdots \sigma^{m-1}(a)}{\sigma(a) \cdot \sigma^2(a) \cdots \underset{a}{\sigma^m(a)}} = 1.$$

To see $\ker(N) \subseteq S$...

Let $\varphi : \mathbb{F}_{q^m}^\times \to \mathbb{F}_{q^m}^\times$ send $\alpha \mapsto \frac{\alpha}{\sigma(\alpha)}$.

Note that $\mathrm{im}(\varphi) = S$, and $\ker(\varphi) = \mathbb{F}_q^\times$.

Since $S \subseteq \ker N$ and $\ker(N)$ has $1 + q + \dots + q^{m-1}$ elements, $S = \ker N$.

6. Let $f = x^4 - 3$. Find the degree of the splitting field of f over $\mathbb{Q}$. Describe the Galois group of f, by giving its action on the roots of f explicitly, and identifying it as isomorphic to a known finite group.

Roots of f: $x^4-3 = (x^2-\sqrt{3})(x^2+\sqrt{3})$
$= (x-\sqrt[4]{3})(x+\sqrt[4]{3})(x-i\sqrt[4]{3})(x+i\sqrt[4]{3})$.

The ratio of any pair of roots is either $1, \pm\sqrt[4]{3}$, or i,
So f splits in $K := \mathbb{Q}(\sqrt[4]{3}, i)$, and since $i \notin \mathbb{Q}(\sqrt[4]{3})$,

$$[\mathbb{Q}(\sqrt[4]{3}, i):\mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt[4]{3}, i):\mathbb{Q}(\sqrt[4]{3})]}_{=2}\underbrace{[\mathbb{Q}(\sqrt[4]{3}):\mathbb{Q}]}_{=4} \text{ so } [K:\mathbb{Q}] = 8.$$

Roots are all $i^j\sqrt[4]{3}$ for $j = 1, 2, 3, 4$.

Then the automorphisms $\sigma = \begin{cases} \sqrt[4]{3} \to i\sqrt[4]{3} \\ i \to i \end{cases}$

and $\tau \begin{cases} \sqrt[4]{3} \to \sqrt[4]{3} \\ i \to -i \end{cases}$

generate $\mathrm{Gal}(K/\mathbb{Q})$. With respect to the ordering
$1 := i\sqrt[4]{3}$, $2 := -\sqrt[4]{3}$, $3 := -i\sqrt[4]{3}$, $4 := \sqrt[4]{3}$
we have $\sigma = (1\ 2\ 3\ 4)$, $\tau = (1\ 3)$,

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