Algebra Qualifying Exam

Naruki Masuda, transcribed by Hui Sun

May 2, 2025

Contents

Chapter 1

Group Theory

1.1 Sylow Theorems

We first talk bout semidirect products. Let G be any group, and N, H be subgroups of G.

Definition 1.1. For $\varphi : H \to \text{Aut}(N)$, define $N \rtimes H$ by

(1) $N \rtimes_\varphi H = N \times H$ as a set.

(b) Equipped with the group structure

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1\varphi(h_1)n_2, h_1h_2)$$

The structure $(N \rtimes_\varphi H, \cdot)$ forms a group.

Example 1.1. If N is a normal subgroup of G, and $N \cap H = \{e\}$, and $\varphi : H \to \text{Aut}(N)$ where

$$\varphi : h \mapsto (n \mapsto hnh^{-1})$$

(acting by conjugation), and $G = NH$. Then

$$N \rtimes_\varphi H \to G$$

where

$$(n, h) \mapsto nh$$

is a bijective homomorphism homomorphism. Hence

$$G \cong N \rtimes_\varphi H$$

Next we present some divisibility results.

Proposition 1.1 (Lagrange, Orbit-Stabilizer). We have the following divisibility results:

- Let H be a subgroup of G, let $[G : H]$ denote the number of cosets of H in G, then

$$|G| = |H|[G : H]$$

- Let G be a finite group acting transitively on a finite set A, then for any $a \in A$, we have

$$|\text{Stab}_G(a)| \cdot |O_G(a)| = |G|$$

The class formula is when G acts on itself by conjugation:

Proposition 1.2 (class formula)**.** Let G act on a finite set S, and let Z denote fixed points of this action, then

$$|S| = |Z| + \sum_{a \in A} |O_G(a)|$$

where A includes exactly one element from each nontrivial orbit.

If G acts on itself by conjugation, then

$$|G| = |Z(G)| + \sum_{g} |[g]| = |Z(G)| + \sum_{g} \frac{|G|}{|C_G(g)|}$$

where $[g]$ denote the conjugacy class of g, and the sum includes exactly one from each nontrivial conjugacy class in G.

Problem 1.1 (F2019-Q2)**.** 2. Let p, q be two prime numbers such that $p \mid q-1$. Prove that

(a) there exists an integer $r \not\equiv 1 \mod q$ such that $r^p \equiv 1 \mod q$;

(b) there exists (up to an isomorphism) only one noncommutative group of order pq.

Proof. (a) We want to show that there exists an element $r \in (\mathbb{Z}/q\mathbb{Z})^\times$ such that

$$r^p \equiv 1 \mod q$$

We can do this because $(\mathbb{Z}/q\mathbb{Z})^\times$ has order $(q-1)$ and $p|(q-1)$. Therefore by Cauchy's theorem, there exists an element of order p in $(\mathbb{Z}/p\mathbb{Z})^\times$.

(b) Let n_p, n_q denote the number of p, q-Sylow subgroups. We see that $n_q|p$ and $n_q \equiv 1 \mod q$, since $p < q$, we must have $n_q = 1$. Now $n_p = 1$ or q by the same reasoning. Suppose $n_q = 1$, let P, Q denote the normal subgroups of order p, q, then

$$G \cong P \times Q$$

by a standard argument (included in the lemma below). Then G is commutative. Since G is noncommutative, we have $n_p = q$. Choose any p-Sylow subgroup P, we know that

$$G \cong Q \rtimes_\theta P$$

where Q is the normal subgroup of order q and $\theta : P \to \mathrm{Aut}(Q) = (\mathbb{Z}/q\mathbb{Z})^\times$. We know either $\theta : 1 \mapsto 1$, is the trivial map which produces a commutative group; or $\theta : 1 \mapsto r$, where $r \in (\mathbb{Z}/q\mathbb{Z})^\times$ is some element of order p.

□

Lemma 1.1. Let p, q be two primes such that $q \nmid (p-1)$, and N, H has order p, q respectively, suppose that N is normal in G, and $N \cap H = \{e\}$, then

$$G \cong N \times H$$

Proof. We consider the map

$$\psi : N \times H \to G$$

such that

$$(n, h) \mapsto nh$$

We want to show that ψ is a homomorphism and ψ is injective (hence bijective by size argument). It is clearly injective:

$$nh = e \Rightarrow n, h \in N \cap H = \{e\}$$

It suffices to show that ψ is a homomorphism. We see that this implies

$$n_1 n_2 h_1 h_2 = n_1 h_1 n_2 h_2$$

Therefore it suffices to for any $n \in N, h \in H$, one has

$$nh = hn$$

Consider the conjugation action

$$\varphi : H \to \text{Aut}(N)$$

where

$$h \mapsto \left(n \mapsto hnh^{-1}\right)$$

Then we claim that φ is trivial. This is because $\ker(\varphi)$ has size either 1 or q. If it has size q, then the map is trivial; if it has size 1, then H embeds in $\text{Aut}(N)$, however, $|H| = q$, $\text{Aut}(N) = p - 1$, and $q \nmid (p-1)$, hence impossible. This shows that the map is trivial, i.e., for $n \in N, h \in H$,

$$hn = nh$$

as desired. □

Problem 1.2 (F2015-Q1)**.** Prove every group of order 15 is cyclic.

Proof. We will show that any group G of order 15 is isomorphic to

$$G \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}}$$

For this, using the above lemma, it suffices to show that there is one normal subgroup of order 3 and one normal subgroup of order 5. We repeat the argument above, $n_5 \mid 3$ and $n_5 \equiv 1 \mod 5$, hence $n_5 = 1$. Moreover, $n_3 \mid 5$ and $n_3 \equiv 1 \mod 3$, hence $n_3 = 1$ as well. By the lemma above, we know that

$$G \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}}$$

hence cyclic as desired. □

Problem 1.3 (S2013-Q2)**.** Let p and q be primes with $p < q$. Let G be a group of order pq. Prove the following statements:

(a) If p does not divide $q - 1$ (i.e., $p \nmid q - 1$), then G is cyclic.

(b) If p divides $q - 1$ (i.e., $p \mid q - 1$), then G is either cyclic or isomorphic to a non-abelian group on two generators. Give the presentation of this non-abelian group.

Proof. This question is exactly the same as F19-Q2, we will only outline here.

(a) We have $n_q = 1$, and $n_p \mid q$, hence $n_p = 1$ or q, moreover $n_p \equiv 1 \mod p$. If $n_p = q$, this implies that $p \mid (q-1)$, hence $n_p = 1$. Therefore by the above argument

$$G \cong \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{q\mathbb{Z}}$$

(b) If $p \mid (q-1)$, then $n_p = 1$ or q. Hence G is either of the form above or isomorphic to the non-abelian group

$$G = Q \rtimes_\theta P$$

We know from F2019-Q2, the trivial θ defines the abelian, hence cyclic group $G = \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{q\mathbb{Z}}$. And $\theta : 1 \mapsto r$, for some $r \in (\mathbb{Z}/q\mathbb{Z})^\times$ of order p defines a non-abelian group. So we have

$$G = \langle g, h : g^q = h^p = e, hgh^{-1} = g^r \rangle$$

□

Problem 1.4 (F2007-Q1). Prove that no group of order 148 is simple.

Proof. We note the prime factorization of 148 is

$$148 = 2^2 \cdot 37$$

We see that $n_{37} \mid 4$ and $n_{37} \equiv 1 \mod 37$, therefore $n_{37} = 1$. This shows that there exists a normal subgroup of order 37, i.e., the group is not simple. □

Problem 1.5 (F2017-Q1). Show that there is no simple group of order 30.

Proof. This is slightly more complicated, and we will use a counting argument. Same reasoning as the above. The prime factorization of 30 is as below:

$$30 = 2 \cdot 3 \cdot 5$$

We see $n_5 \mid 6$, and $n_5 \equiv 1 \mod 5$. Unfortunately, n_5 could either be 1 or 6. Now $n_3 \mid 10$, and $n_3 \equiv 1 \mod 3$, unfortunately again n_3 could be 10. However, we argue that $n_3 = 10$ and $n_5 = 6$ cannot happen at the same time. Suppose this is the case, then there are 20 elements of order 2 and 24 elements of order 5, but this is too many! Hence either $n_3 = 1$ or $n_5 = 1$, as desired. □

Problem 1.6 (F2011-Q1).

(a) Let G be a group of order 5046. Show that G cannot be a simple group. You may not appeal to the classification of finite simple groups.

(b) Let p and q be prime numbers. Show that any group of order p^2q is solvable.

Proof. The proof is very similar like above.

(a) The prime factorization of 5049 is as follows:

$$5049 = 2 \cdot 3 \cdot 29^2$$

Hence we see $n_{29} = 1$, i.e., there is a normal subgroup of order 29, therefore not simple.

(b) We will do discussion by cases.

(1) $p > q$. Then $n_p = 1$ or q and $n_p \equiv 1 \mod p$, therefore $n_p = 1$. Let P be the normal subgroup of G of order p^2, we thus have

$$\{e\} \subset P \subset G$$

It is clear that $|G/P| = q$, thus abelian, and $|P| = p^2$ also abelian as well (by the lemma below). This shows that G is solvable.

(2) $p < q$. Then $n_p = 1$ or q, and $n_q = 1$ or p^2. Suppose that $n_q = 1$, let Q denote the normal subgroup of order q, then

$$\{e\} \subset Q \subset G$$

It is clear that Q and G/Q are both abelian. Suppose that $n_q = p^2$ instead, then there are only $p^2q - p^2(q-1) = p^2$ elements of order $\neq q$. Since any p-Sylow subgroup has p^2 elements with order $\neq q$, we must have $n_p = 1$. Hence we are in case (1) again. This shows that G is solvable in either case $n_q = 1, p^2$.

□

Lemma 1.2 (p^2 abelian). Fix prime p, any group of order p^2 is abelian.

Proof. For any nontrivial p group, by the class formula, the center $Z(G)$ is nontrivial, thus the center has order either p or p^2. If it has order p^2, then the group is abelian. If it has order p, then

$$|G/Z(G)| = p$$

is also cyclic, therefore G is abelian (strictly speaking is a contradiction that $|Z(G)| = p$). In either case, we see that G is abelian. □

Problem 1.7. Any p-group is solvable, for any prime p.

Proof. Suppose $|G| = p^r$ for some $r \geq 0$, we will use induction on r. If $r = 0$, then the trivial group is trivally solvable.

- Base case: if $r = 1$, $|G| = p$, then G is cyclic, hence solvable.
- Induction step: suppose that G is solvable for all $|G| = p^k$, where $0 \leq k \leq r-1$. Now we want to show that G of order p^r is solvable. We know G has a nontrivial center, suppose that $|Z(G)| = p^k$, where $1 \leq k \leq r$, then

  $$|G/Z(G)| = p^{r-k}, 0 \leq r-k \leq r-1$$

  We know any group G is solvable if and only if there exists a sequence of subgroups $G_0, \ldots, G_k$

  $$\{e\} = G_0 \subset \cdots \subset G_k = G$$

  such that G_{i-1} is normal in G_i and G_i/G_{i-1} is solvable. Therefore we see when $|G| = p^r$,

  $$\{e\} \subset Z(G) \subset G$$

  has $Z(G)$ solvable, and $G/Z(G)$ also solvable by the induction hypothesis, so we close the induction.

□

Problem 1.8 (S2016-Q1). Classify all groups of order 66, up to isomorphism.

Proof. By $66 = 2 \cdot 3 \cdot 11$, we know $n_{11} = 1$. We claim that there is a normal subgroup isomorphic to $\mathbb{Z}/33\mathbb{Z}$.

1. First we show that there is a subgroup of order 33. Let P_{11} denote the normal subgroup of order 11 and let P_3 denote a 3-Sylow subgroup of G. Then we claim that the following

   $$H = \{gh : g \in P_{11}, h \in P_3\}$$

   forms a subgroup and is isomorphic to $\mathbb{Z}/33\mathbb{Z}$. By the Lemma 1.1, we see that

   $$H \cong \frac{\mathbb{Z}}{11\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} = \frac{\mathbb{Z}}{33\mathbb{Z}}$$

2. Now we show that it is normal. This follows from the following general lemma:

> **Lemma 1.3.** Let p be the smallest prime factor of $|G|$, and let H be a subgroup with index p, then H is normal.

Proof. We will only prove in the case that H is a subgroup of index 2, i.e., $G = H \sqcup (G \setminus H)$. We see for all $g \in G$,

$$gH = Hg$$

since if $g \in H$, then the equality holds; if $g \notin H$, then $gH = G \setminus H$, so is Hg. □

Now since there is a subgroup of order 2, we can write G as a semidirect product

$$G = \frac{\mathbb{Z}}{33\mathbb{Z}} \rtimes_\theta \frac{\mathbb{Z}}{2\mathbb{Z}}$$

The number of nonisomorphic groups will depend on the choice of θ. There are four different choices for $\theta : H \to \mathrm{Aut}\left(\frac{\mathbb{Z}}{11\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}\right) = \frac{\mathbb{Z}}{10\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$

$$\begin{cases} \theta_1 : 1 \mapsto (0,0) \\ \theta_2 : 1 \mapsto (0,1) \\ \theta_3 : 1 \mapsto (5,0) \\ \theta_4 : 1 \mapsto (5,1) \end{cases}$$

There are 4 different groups and one can write them in cyclic notation using the θ above. □

> **Problem 1.9** (S2007-Q2). Prove that no group of order 224 is simple.

Proof. The prime factorization is

$$224 = 2^5 \cdot 7$$

If $n_2 = 1$ or $n_7 = 1$, then we are done; assume that $n_2 = 7$ instead, then we recall G has a nontrivial transitive action on the set of 2-Sylow subgroups, i.e., there is a homomorphism $\varphi : G \to S_7$. We know $\ker(\varphi)$ is a normal subgroup of G. Since the action is nontrivial transitive, we know $\ker(\varphi) \neq G$. If $\ker(\varphi) = \{e\}$, then φ produces an embedding of G into S_7. However, $|G| = 224 \nmid |S_7|$. This shows that $\ker(\varphi)$ is a nontrivial proper normal subgroup of G, concluding that G is not simple. □

> **Problem 1.10** (F2008-Q1). Show that no group of order 36 is simple.

Proof.

$$36 = 2^2 \cdot 3^3$$

We know $n_2 \mid 9, n_2 \equiv 1 \mod 2$, and $n_3 \mid 4, n_3 \equiv 1 \mod 3$. We know $n_3 = 1$ or 4, suppose that $n_3 = 4$, then there is a nontrivial action of G on the set of 3-Sylow subgroups, i.e.,

$$\varphi : G \to S_4$$

Suppose that G is simple, we know $\ker(\varphi) \neq G$ since the action is nontrivial, by assumption $\ker(\varphi) = \{e\}$, which implies that φ is an embedding, but $|G| = 32 \nmid |S_4|$, which is a contradiction. This implies that G is not simple. □

Problem 1.11 (S2014-Q2). All groups of order less than 60 are solvable, i.e., there exists a sequence of subgroups of G, $G_0, \ldots, G_k$ such that G_i is normal in G_{i+1} and G_{i+1}/G_i is abelian, and

$$1 = G_0 \subset \cdots \subset G_k = G$$

Proof. Groups of order p, pq, p^2, p^2q are solvable.

$$\{1,2,3,4,5,6,7,9,10,11,12,13,14,15,17,19,20,21,22,23,25,26,28,29,30,$$
$$31,33,34,35,37,38,39,41,43,44,45,46,47,49,50,51,52,53,55,57,58,59\}$$

And any p-group is also solvable.

$$\{8,16,27,32\}$$

The remaining groups are

$$\{24,36,40,42,48,54,56\}$$

24: If $n_2 = 1$ or $n_3 = 1$, then we are done. We see $n_2 = 1$ or 3, consider the action $\varphi : G \to S_3$. We see $\ker(\varphi)$ is a proper normal subgroup of G, this implies that

$$\{e\} \subset \ker(\varphi) \subset G$$

where $|\ker(\varphi)|$ is a known solvable group, hence we are done.

36: Exactly same as above, we assume $n_3 \neq 1$, therefore $n_3 = 4$, the action $\varphi : G \to S_4$ is not injective, hence $\ker(\varphi)$ is again a proper normal subgroup of G that is solvable.

40: We see $n_5 = 1$, therefore

$$\{e\} \subset \mathbb{Z}/5\mathbb{Z} \subset G$$

42: We see $n_7 = 1$.

48: We see $n_2 = 1$ or 3, the the action $\varphi : G \to S_3$ is not injective, hence $\ker(\varphi)$ is a proper normal subgroup of G that is solvable.

54: We see $n_3 = 1$.

56: We know $n_7 = 1$ or 8 and $n_2 = 1$ or 7. The group action argument does not work. We assume $n_7 = 8$, then there can be at most $56 - 8(7-1) = 8$ elements of order $\neq 7$. This shows that $n_2 = 1$. Hence

$$\{e\} \subset P_2 \subset G$$

$\square$

Problem 1.12 (S2012-Q1). Let G be a group of order p^3q^2, where p and q are prime integers. Show that for p sufficiently large and q fixed, G contains a normal subgroup other than $\{1\}$ and G.

Proof. We want to show that there exists a normal group of size p^3, i.e., $n_p = 1$. We know $n_p \mid q^2, n_p \equiv 1 \mod p$. Let p be large enough such that $p > (q^2 - 1)$, then ths forces $n_p = 1$, as desired. $\square$

Problem 1.13 (F2014-Q4).

(a) Let G be a group of order p^2q^2, where p and q are distinct odd primes, with $p > q$. Show that G has a normal subgroup of order p^2.

(b) Can a solvable group contain a non-solvable subgroup? Explain.

Proof. (a) We know $n_p = 1$ or q or q^2, and $n_p \equiv 1 \mod p$. Since $p > q$, we know $n_p \neq q$. It suffices to show that $n_p \neq q^2$: suppose that $n_p = q^2$, then

$$p \mid (q^2 - 1) = (q+1)(q-1)$$

Since p is prime, $p \mid (q+1)$ or $p \mid (q-1)$. The latter impossible since $q < p$. $p \mid (q+1)$ is also impossible because this implies that $q = p+1$, which implies that q is even, a contradiction.

(b) It is not possible. Suppose G is a solvable group, let H be a subgroup of G, then we know there exists sequence

$$\{e\} = G_0 \subset \cdots \subset G_k = G$$

such that G_i is normal in G_{i+1} and $\frac{G_{i+1}}{G_i}$ is abelian. We define $H_i = G_i \cap H$, then we see H is solvable with sequence $H_0 \subset \ldots H_k$.

□

Problem 1.14 (F2018-Q2)**.** Let G be a group of order 24. Assume that no Sylow subgroup of G is normal in G. Show that G is isomorphic to the symmetric group S_4.

Proof. By Sylow, we have $n_3 = 4, n_2 = 3$. Denote $\text{Syw}_3(G) = \{P_1, P_2, P_3, P_4\}$ and consider the transitive action by of G by conjugation on this set, which embeds in S_4, i.e., $\varphi : G \to S_4$. By a size argument, it suffices to show that φ is injective. We see that

$$\ker(\varphi) = \{g \in G : gP_ig^{-1} = P_i \text{ for each } i\} = \bigcap_{i=1}^{4} N_G(P_i)$$

By the orbit-stabilizer theorem, $|N_G(P_i)| = 6$ for all i. However, for any $i \neq j$, 3 does not divide $|N_G(P_i) \cap N_G(P_j)|$: if not, the intersection would include a 3-Sylow subgroup but P_i is the only 3-Sylow subgroup in $N_G(P_i)$, thus this is impossible. It remains to see that $|\ker(\varphi)| \neq 2$. Suppose that it is, then $\operatorname{im}(\varphi)$ is an index 2 subgroup of S_4, hence

$$\frac{G}{\ker \varphi} \cong A_4$$

and $K = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is normal in A_4, hence so is $\varphi^{-1}(K)$ (it has size 8) in G. This is a contradiction because this implies there is a normal 2-Sylow subgroup. □

Problem 1.15 (F2001-Q1)**.** Let G be a finite group and let N be a normal subgroup of G such that N and G/N have relatively prime orders.

1. Assume that there exists a subgroup H of G having the same order as G/N. Show that $G = HN$. (Here HN denotes the set $\{xy \mid x \in H, y \in N\}$.)
2. Show that $\phi(N) = N$, for all automorphisms ϕ of G.

Proof. 1. Since N, H have relatively prime orders, $N \cap H = \{e\}$, thus we can write

$$G = N \rtimes_\theta H$$

where $\theta(h)n = hnh^{-1}$. One can show that the map $\varphi : N \rtimes_\theta H \to G$ as

$$\varphi : (n, h) \mapsto nh$$

It is clear that φ is a homomorphism and injective, thus by a size argument we have φ is an isomorphism. This shows $G = NH$ and similarly $G = HN$.

2. Any automorphism ϕ of G permutes the p-Sylow subgroups. Suppose that $|G| = p_1^{i_1} \dots p_k^{i_k}$, then after rearranging,
$$|N| = p_1^{i_1} \dots p_j^{i_j}$$
because N and G/N have relatively prime orders. Hence N contains all the Sylow p_i-subgroups, hence $\phi(N) = N$ for all automorphisms ϕ of G.

□

Problem 1.16 (S2001-Q1). Let G be a finite group and p the smallest prime number dividing the order $|G|$ of G. Let H be a subgroup of G of index p in G. Show that H is necessarily a normal subgroup of G.

Proof. G has an action on G/H by left multiplication: $\varphi : G \to \text{Aut}(G/H)$ such that
$$\varphi(g)(\bar{g}H) = g\bar{g}H$$
We will show that $H = \ker(\varphi)$. First we see that $\ker(\varphi) \subset H$:
$$\ker(\varphi) = \{g \in G : g\bar{g}H = \bar{g}H : \text{ for all } \bar{g} \in G\}$$
letting $\bar{g} \in H$ we see $g \in \ker(\varphi)$ implies $g \in H$, i.e., $\ker(\varphi) \subset H$.

Now we use a size argument to show $|H| \leq |ker\varphi|$. We note that $\text{im}(\varphi)$ is a subgroup of $\text{Aut}(G/H) = S_p$, thus
$$\frac{|G|}{|\ker(\varphi)|} \text{ divides } p!$$
because $\frac{|G|}{|\ker(\varphi)|}$ also divides $|G|$ and p is the smallest prime that divides p, we must have
$$\frac{|G|}{|\ker(\varphi)|} \text{ divides } p$$
Note that $\frac{|G|}{|H|} = p$, this gives
$$|H| \leq |\ker(\varphi)|$$
which shows $H \subset \ker(\varphi)$, hence $H = \ker(\varphi)$. □

(End of Page 5)

1.2 Class Formula, Classification of p-groups

Definition 1.2 (nilpotent group). Let G be a group. Define inductively an increasing sequence $\{e\} = Z_0 \subseteq Z_1 \subseteq Z_2 \subseteq \cdots$ of subgroups of G as follows: for $i \geq 1$, Z_i is the subgroup of G corresponding to the center of G/Z_{i-1}. One can show that Z_i is normal in G. A group is *nilpotent* if $Z_m = G$ for some m.

Example 1.2.

- p-groups are nilpotent.
- Nilpotent groups are solvable.

Proposition 1.3. We have the following classification of groups of order p, p^2, p^3, for prime p.

- $|G| = p$ implies $G \cong \mathbb{Z}/p\mathbb{Z}$.
- $|G| = p^2$ implies
$$G \cong \frac{\mathbb{Z}}{p^2\mathbb{Z}} \quad \text{or} \quad G \cong \frac{\mathbb{Z}}{p\mathbb{Z}} \oplus \frac{\mathbb{Z}}{p\mathbb{Z}}$$
- $|G| = p^3$ implies that
$$G \cong \frac{\mathbb{Z}}{p^3\mathbb{Z}} \quad \text{or} \quad G/Z(G) \cong \frac{\mathbb{Z}}{p\mathbb{Z}} \oplus \frac{\mathbb{Z}}{p\mathbb{Z}} \quad \text{or} \quad [G,G] = Z(G)$$

Problem 1.17 (S2010-Q1). Let G be a non-abelian group of order p^3, where p is prime. Determine the number of distinct conjugacy classes in G.

Proof. We know G has a nontrivial center, and if $|Z(G)| = p^2$ or p^3, then G is abelian, this shows that $|Z(G)| = p$, now let $g \in G \setminus Z(G)$, then
$$Z(G) \subsetneq Z_g(G) \subsetneq G$$
where $Z(G) \subsetneq Z_g(G)$ because $g \in Z_g(G)$, and $Z_g(G) \subsetneq G$ since $g \notin Z(G)$. This shows that $Z_g(G)$ is a subgroup of order p^2, in other words, the size of the conjugacy class of any $g \in G \setminus Z(G)$ is
$$|[g]| = \left| \frac{G}{Z_g(G)} \right| = p$$
By the class formula,
$$|G| = |Z(G)| + \sum_{a \in A} |[a]|$$
where A contains one a from each nontrivial conjugacy class $[a]$. Thus we have
$$p^3 = p + Np \Rightarrow N = p^2 - 1$$
Every element in $Z(G)$ is its own conjugacy class, thus the total number of conjugacy classes is
$$p^2 + p - 1$$
□

Problem 1.18 (F2013-Q1). Let $p > 2$ be a prime. Classify groups of order p^3 up to isomorphism. The two nonabelian groups of order p^3 (for $p \neq 2$), up to isomorphism, are:
$$\mathrm{Heis}(\mathbb{Z}/(p)) = \left\{ \left(\begin{array}{ccc} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{array} \right) \middle| a, b, c \in \mathbb{Z}/(p) \right\}$$
and
$$\begin{aligned} G_p &= \left\{ \left(\begin{array}{cc} a & b \\ 0 & 1 \end{array} \right) \middle| a, b \in \mathbb{Z}/(p^2), a \equiv 1 \bmod p \right\} \\ &= \left\{ \left(\begin{array}{cc} 1+pm & b \\ 0 & 1 \end{array} \right) \middle| m, b \in \mathbb{Z}/(p^2) \right\} \end{aligned}$$

Problem 1.19 (F2014-Q5).

(a) Prove that every group of order p^2 (with p prime) is abelian. Then classify such groups up to isomorphism.

(b) Give an example of a non-abelian group of order p^3 for $p = 3$.
Suggestion: Represent the group as a group of matrices.

Proof. (a) See Lemma 1.2. There are two abeliean groups: $\frac{\mathbb{Z}}{p^2\mathbb{Z}}, \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}$.

(b) See Problem 1.18.

□

Problem 1.20 (F2019-Q4, S2015-Q3). Find all irreducible representations of a finite p-group over a field of characteristic p.

Proof. Let G any finite p-group. Let V be an irreducible representation over $\mathbb{F}_p$, consider the $[\mathbb{F}_pG]$-module W generated by any $v \in V \setminus \{0\}$. We see W is a finite-dimensional vector space over $\mathbb{F}_p$, i.e.,

$$|W| = p^d$$

for some $d \geq 1$. We consider the action of G on W, all the orbits of this action either has size 1 or is a power of p, since G is a p-group, by the class formula, let N be the number of nontrivial orbits of size 1,

$$|W| \equiv 1 + N \mod p \Rightarrow 1 + N \equiv 0 \mod p$$

Hence there exists at least one nontrivial orbit $\{v\}$ of size 1. We consider the vector space $\bar{W}$ generated by v over $\mathbb{F}_p$: it is one-dimensional vector space contained in V, invariant under G, since V is irreducible, we must have $V = \bar{W}$. The action of G on $\bar{W}$ is the trivial action, thus all irreducible representations of a finite p-group over $\mathbb{F}_p$ are trivial. □

1.3 Random Problems

Problem 1.21 (F2010-Q1). Let G be a group. Let H be a subset of G that is closed under group multiplication. Assume that $g^2 \in H$ for all $g \in G$. Show that:

- H is a normal subgroup of G
- G/H is abelian

Proof.
- We first show that H is subgroup. It remains to show that if $h \in H$, then $h^{-1} \in H$, we know $(h^{-1})^2 \in H$, thus

$$h(h^{-1})^2 = h^{-1} \in H$$

as desired. Now we show that H is normal: for any $h \in H$, $g \in G$, we want to show $ghg^{-1} \in H$.

$$\begin{aligned} ghg^{-1} &= (gh)^2(gh)^{-1}hg^{-1} \\ &= (gh)^2h^{-1}g^{-1}hg^{-1} \\ &= (gh)^2h^{-1}(g^{-1}h)^2(g^{-1}h)^{-1}g^{-1} \\ &= (gh)^2h^{-1}(g^{-1}h)^2h^{-1} \in H \end{aligned}$$

as desired.

- It suffices to show that for any $g_1, g_2 \in G$, we have

$$g_1 g_2 H \subset g_2 g_1 H$$

Take any $h \in H$, we want to show $(g_2g_1)^{-1}g_1g_2h \in H$,

$$\begin{aligned}(g_2g_1)^{-1}g_1g_2h &= (g_2g_1)^{-2}g_2g_1^2g_2h \\ &= (g_2g_1)^{-2}(g_2g_1^2)^2(g_2g_1^2)^{-1}g_2h \\ &= (g_2g_1)^{-2}(g_2g_1^2)^2g_1^{-2}h \in H\end{aligned}$$

as desired.

□

Problem 1.22 (S2014-Q1). Find the number of colorings of the faces of a cube using 3 colors, where two colorings are considered equal if they can be transformed into each other by a rotation of the cube.

[*Hint*: Use Burnside's formula:

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g|,$$

where a group G acts on a set X, X/G is the set of orbits, and for every $g \in G$, X^g is the fixed subset of g in X.]

Proof. Let X be the set of all possible colorings of the cube (equal cubes allowed), we have $|X| = 3^6$. We notice two things:

1. The group of rotations of a cube is S_4.
2. For $\sigma_1, \sigma_2 \in S_4$ that are conjugates of each other, $|X^{\sigma_1}| = |X^{\sigma_2}$. Therefore for the Burnside's formula becomes

$$|X/S_4| = \frac{1}{|S_4|}\sum_{[\sigma] \text{ conj classes}} |[\sigma]| \cdot |X^\sigma|$$

Now we analyze for each conjugacy class $[\sigma]$, what is $|X^\sigma|$.

- $(1+1+1+1)$, $|[e]| = 1$ and $|X^e| = 3^6$.
- $(1+1+2)$, $|[\sigma_1]| = 6$ and $|X^{\sigma_1}| = 3^3$.
- $(1+3)$, $|[\sigma_2]| = 8$, and $|X^{\sigma_2}| = 3^2$.
- $(2+2)$, $|[\sigma_3]| = 6$, and $|X^{\sigma_3}| = 3^4$.
- (4), $|[\sigma_4]| = 6$, and and $|X^{\sigma_4}| = 3^3$.

Thus combining we get

$$|X/S_4| = \frac{1}{24}\left(3^6 + 6\cdot 3^3 + 8\cdot 3^2 + 6\cdot 3^4 + 6\cdot 3^3\right) = 57$$

□

Problem 1.23 (S2019-Q4). Let f be a polynomial with n variables and define

$$\mathrm{Sym}(f) = \{\sigma \in S_n \mid f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f(x_1, x_2, \ldots, x_n)\}.$$

1. Prove that $\mathrm{Sym}(f)$ is a subgroup of S_n.
2. Prove that the dihedral group D_4 (the group of symmetries of the square) is isomorphic to $\mathrm{Sym}(x_1x_2 + x_3x_4)$.

Proof. 1. The group S_n acts on the polynomial ring $k[x_1, \ldots, x_n]$, by permuting the x_i to $x_{\sigma(i)}$, and we see that Sym(f) is the centralizer of a fixed element $f \in k[x_1, \ldots, x_n]$, hence is a subgroup.

2. We have a total of 8 elements in Sym($x_1x_2 + x_3x_4$):

$$\{e, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}$$

and we can by drawing a square tha this corresponds to the group D_4.

□

Problem 1.24 (S2011-Q1, F2004-Q1).

(a) Let H be a proper nontrivial subgroup of a finite group G (i.e., $H \neq \{1\}$ and $H \neq G$). Prove that G is not the union of all conjugates of H in G.

(b) Give an example of an infinite group G for which the assertion in part (a) fails.

Proof. (a) If H is normal, then all conjugations of H is equal to H, but $H \subsetneq G$, this G is not not the union of all conjugates of H in G. Now suppose H is not normal, assume the contrary that G is the union of all conjugates of H, then the number of distinct conjugates of H is $[G : N_G(H)]$, hence

$$|G| = [G : N_G(H)] \cdot |H| \iff [G : H] = [G : N_G(H)] \iff [N_G(H) : H] = 1$$

this is a contradiction since H is not normal. Thus G not the union of all conjugates of H in G.

(b) Consider

$$B = \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\} \subset \mathrm{GL}_2(\mathbb{C})$$

It is clear that conjugation of matrices in B do not give matrices with nonzero left bottom entry.

□

Problem 1.25 (S2009-Q1). Let H and K be two solvable subgroups of a group G such that $G = HK$.

1. Show that if either H or K is normal in G, then G is solvable.
2. Give an example where G may not be solvable without the assumption in (a).

Proof. 1. WLOG suppose that H is normal, then the composite map $\varphi = \pi \circ \iota$:

$$K \xrightarrow{\iota} G \xrightarrow{\pi} G/H$$

is surjective, therefore

$$\{e\} \subset H \subset G$$

$G/H \cong K/\ker(\varphi)$ is solvable, hence G is solvable.

2. The smallest nonsolvable group is A_5, we have
$$A_5 = HK$$
where $H = \langle(12345)\rangle, K = A_4 = \{\sigma \in A_5 : \sigma(5) = 5\}$. Now H, K are both solvable, but G is not.

$\square$

Problem 1.26 (F2003-Q1). In a group G, let 1 denote the identity element and let $[x, y] = xyx^{-1}y^{-1}$ denote the commutator of elements $x, y \in G$.

1. Express $[z, xy]x$ in terms of x, $[z, x]$, and $[z, y]$.
2. Prove that if the identity $[[x, y], z] = 1$ holds in G, then the following identities hold in G:
$$[x, yz] = [x, y][x, z] \quad \text{and} \quad [xy, z] = [x, z][y, z].$$

Proof. 1. We have
$$\begin{aligned}[z, xy]x &= zxyz^{-1}y^{-1}x^{-1}x \\ &= zxz^{-1}x^{-1}xzyz^{-1}y^{-1} \\ &= [z, x]x[z, y]\end{aligned}$$

2. The identity $[[x, y], z] = 1$ implies
$$[x, y]z = z[x, y]$$
Therefore using the identity in 1, we have
$$\begin{aligned}[x, yz] &= [x, y]y[x, z]y^{-1} \\ &= [x, y]yy^{-1}[x, z] \\ &= [x, y][x, z]\end{aligned}$$
Similarly
$$\begin{aligned}[xy, z] &= xyzy^{-1}x^{-1}z^{-1} \\ &= xyzy^{-1}z^{-1}zx^{-1}z^{-1} \\ &= x[y, z]x^{-1}[x, z] \\ &= [y, z][x, z] \\ &= [x, z][y, z]\end{aligned}$$

$\square$

Problem 1.27 (S2005-Q1). Let k be a field. Let $G = \mathrm{GL}_n(k)$ be the general linear group, where $n > 0$. Let D be the subgroup of diagonal matrices, and let $N = N_G(D)$ be the normalizer of D in G. Determine the quotient group N/D.

Problem 1.28 (F2009-Q1). Let G be a finite group, and let $\mathrm{Aut}(G)$ be its automorphism group. Consider the group action $\phi\colon \mathrm{Aut}(G) \times G \to G$ defined by $\phi(\sigma, g) = \sigma(g)$. Assume G has exactly two orbits under this action.

1. Determine all such groups G up to isomorphism.
2. For each case from (a), determine when $\mathrm{Aut}(G)$ is solvable.

Problem 1.29 (F2016-Q1)**.** Determine $\mathrm{Aut}(S_3)$.

Proof. Every element $\sigma \in \mathrm{Aut}(S_3)$ must send order 2 elements $\{(12), (23), (13)\}$ to one another, and order 3 elements $\{(123), (132)\}$ to each other. However, σ is determined by how it permutes

$$\{(12), (23), (13)\}$$

Thus every σ is an inner automorphism of the form $\sigma_g(h) = ghg^{-1}$ for $g, h \in S_3$ and g is some transposition. Hence

$$\mathrm{Aut}(S_3) \cong S_3$$

$\square$

Chapter 2

Representation Theory

Proposition 2.1 (properties of characters)**.**

Proposition 2.2. The character tables for S_3, S_4, A_5, S_5 are as follows:

Theorem 2.1 (Compilation of theorems)**.** Schur's lemma:

1. If $\varphi : V \to W$ is a G-invariant map, i.e.,
$$\varphi(\rho(g)(v)) = \rho(g)\varphi(v)$$
where V, W are irreducible representations, then $\varphi = 0$ or an isomorphism. This is true for any field k that V, W are over.

2. If $\varphi : V \to V$ and everything as above, then
$$\varphi(v) = \lambda v$$
for some $\lambda \in k^\times$. This is only true when k is algebraically clsoed.

3. $\mathrm{Hom}_G(V, W) \begin{cases} k \text{ if } V \cong W \\ 0 \text{ if not} \end{cases}$, where V, W are irreducible. This is true for k algebraically closed.

4. Mascheke's theorem: any finite dimensional representation V of a finite group G can be decomposed into a direct sum of irreducible representations.
$$V = V_1^{r_1} \oplus \cdots \oplus V_k^{r_k}$$
where V_i's are irreducible. This is true when the characteristic k does not divide $|G|$, notably this always holds for characteristic 0 fields.

5. Do not mix them up.

Proposition 2.3. G is abelian if and only if every irreducible representation ρ is one-dimensional.

Proof. If G is abelian, take any irreducible representation ρ,
$$\{\rho(g) : g \in G\}$$

can be simultaneously diagonalized (minimal polynomial has no repeated factor), i.e., there exists an eigenbasis $\{e_1, \ldots, e_n\}$ such that $\rho(g)$ is a diagonal matrix for all g. This implies that the vector space generated by $\{e_i\}$ for each i is a ρ-invariant subspace, since ρ is irreducible, ρ must be one-dimensional.

Conversely, let $|G| = n$, if every irreducible ρ is one-dimensional, then there are n irreducible representations, i.e., n conjugacy classes, i.e., G is abelian. □

2.1 Characters

Problem 2.1 (S2008-Q4). Let $V \cong \mathbb{C}^n$ be an n-dimensional complex vector space with standard basis $e_1, \ldots, e_n$. Consider the permutation action $S_n \times V \to V$ defined by:

$$\sigma \cdot e_i = e_{\sigma(i)} \quad \text{for } \sigma \in S_n$$

Decompose V into irreducible $\mathbb{C}[S_n]$-modules.

Problem 2.2 (S2014-Q5). Find the table of characters for S_4.

Problem 2.3 (F2016-Q6). Find a table of characters for the alternating group A_5.

Problem 2.4 (F2015-Q3). Let $G = S_4$ (the symmetric group on four letters).

(a) Prove that G has two non-equivalent irreducible complex representations of dimension 3; call them ρ_1 and ρ_2.

(b) Decompose the tensor product representation $\rho_1 \otimes \rho_2$ into a direct sum of irreducible representations of G.

Problem 2.5 (F2011-Q4). Let $\rho\colon S_3 \to \mathrm{GL}(2, \mathbb{C})$ be a two-dimensional irreducible representation of the symmetric group S_3.

1. Decompose the tensor square $\rho^{\otimes 2}$ into irreducible representations of S_3.
2. Decompose the tensor cube $\rho^{\otimes 3}$ into irreducible representations of S_3.

Problem 2.6 (F2014-Q3). Let $G = S_3$ be the symmetric group on three elements.

(a) Prove that G has an irreducible complex representation of dimension 2 (call it ρ), but none of higher dimension.

(b) Decompose the triple tensor product $\rho \otimes \rho \otimes \rho$ into a direct sum of irreducible representations of G.

Problem 2.7 (S2006-Q6). Let S_4 be the symmetric group on four elements.

1. Give an example of a non-trivial 8-dimensional complex representation of S_4.
2. Show that every 8-dimensional complex representation of S_4 contains a 2-dimensional invariant subspace.

Problem 2.8 (F2007-Q5). Prove that every 5-dimensional complex representation of the alternating group A_4 (the alternating group of degree 4) contains a 1-dimensional invariant subspace.

Problem 2.9 (S2004-Q6). Consider complex representations of a finite group G. Let $\sigma_1, \dots, \sigma_s$ be representatives of the conjugacy classes of G, and let $\chi_1, \dots, \chi_s$ be the irreducible characters of G.

1. Define an inner product on the $\mathbb{C}$-vector space of class functions on G such that $\{\chi_1, \dots, \chi_s\}$ forms an orthonormal basis.
2. Let $A = (a_{ij})$ be the character table matrix of G, where $a_{ij} = \chi_i(\sigma_j)$ for $1 \le i, j \le s$. Prove that A is invertible.

Problem 2.10 (S2018-Q4, S2007-Q5). Is S_4 isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{C})$?

Problem 2.11 (S2010-Q6). Let G be a group of order 24. Using representation theory, prove that $G \neq [G, G]$, where $[G, G]$ denotes the commutator subgroup of G.

Proof. Suppose $G = [G, G]$, then we claim the only 1-dimensional representation $\rho : G \to \mathbb{C}^\times$ is the trivial one. This is because if ρ is one-dim, then

$$[G, G] \subset \ker(\rho)$$

i.e., ρ is trivial. However, there is no way to write

$$|G| = 24 = 1 + d_1^2 + \cdots + d_k^2$$

where $d_i \ge 2$. Thus $G \neq [G, G]$. □

Problem 2.12 (F2017-Q6). Let G be a finite group with center $Z(G)$. Show that if G admits a faithful irreducible representation $\rho\colon G \to \mathrm{GL}_n(k)$ for some positive integer $n \in \mathbb{Z}^+$ and some field k, then the center $Z(G)$ is cyclic.

Proof. (We will only do the case where k is algebraically closed). For any $z \in Z(G)$, $\rho(z) : V \to V$ is a G-map, i.e.,

$$\rho(z)(\rho(g)v) = \rho(g)(\rho(z)v)$$

We know by Schur's lemma that $\rho(z)$ is a scalar multiplication:

$$\rho(z) \in k^\times$$

Because ρ is faithful, Z embeds into $k^\times$ via ρ.

Lemma 2.1 (Fact). Any finite subgroup of $k^\times$ for field k is cyclic.

Hence Z is cyclic. □

Problem 2.13 (S2005-Q6). Let V be a finite-dimensional vector space over a field k, and let G be a finite group with an irreducible representation $\varphi\colon G \to \mathrm{GL}(V)$. Suppose H is a finite abelian subgroup of $\mathrm{GL}(V)$ contained in the centralizer of $\varphi(G)$. Prove that H must be cyclic.

Proof. Just like above, we embed H into $k^\times$. Let any $h \in H$, we note that h is a G-map, i.e., for any $g \in G$,

$$h(\varphi(g)v) = \varphi(g)hv$$

this is because h is contained in the centralizer of $\varphi(G)$, i.e., commutes with all $\varphi(g)$. By Schur's Lemma, we have

$$h = \lambda I, \text{ where } \lambda \in k^\times$$

One can define a homomorphism $\psi : H \to k^\times$ such that

$$\psi(\lambda I) = \lambda$$

This map embeds H into $k^\times$, and we are done by again observing any finite subgroup of $k^\times$ is cyclic, □

Problem 2.14 (F2010-Q6). Let G be a non-abelian group of order p^3, where p is prime.

1. Determine the number of isomorphism classes of irreducible complex representations of G, and find their dimensions.
2. Which of these irreducible complex representations are faithful? Justify your answer.

Proof.

1. In S2010-Q1, we showed there are p^2-1+p conjugacy classes in a non-abelian group G of order p^3. There are p^2 one-dimensional irreducible representations because one dimensional representations of G are equivalent to one-dimensional representations of $G/[G,G]$ which has size p^2, thus abelian and all irreducible representations are one-dimensional.

   Lemma 2.2 (Fact). Let V be an irreducible representation, then $\dim V$ divides $|G|$. (This is true when k is algebraically closed and characteristic 0).

   Thus it is clear that there are $p-1$ representations of dimension p. (Sanity check: $|G| = p^3 = p^2 + (p-1)p^2$).

2. We claim that all the one-dimensional representations are not faithful and all the p-dimensional representations are. Recall ρ is irreducible if and only if $\ker(\rho) = \{g : \rho(g)v = v \text{ for all } v\} = \{e\}$.

   Lemma 2.3 (Fact). Let $\rho : G \to \mathbb{C}^\times$ be a one-dimensional irreducible representation, then

   $$[G,G] \subset \ker(\rho)$$

   Thus if ρ is one-dimensional, then ρ is not faithful. Now for the higher dimensional case:

   Lemma 2.4 (Fact). If $\rho : G \to \mathrm{GL}_p(\mathbb{C})$ is an irreducible representation, then $\bar{\rho} : \frac{G}{\ker \rho} \to \mathrm{GL}_p(\mathbb{C})$ is also irreducible.

   If $\ker \rho$ is nontrivial, then it must divide the size of $|G|$, hence $\frac{G}{\ker \rho}$ is abelian, i.e., all irreducible representations are one-dimensional. This is a contradiction since ρ is p-dimensional, thus $\ker(\rho) = \{e\}$, as desired.

□

Problem 2.15 (S2011-Q5). Let K be a field, and let $\Phi\colon G \to \mathrm{GL}_n(K)$ be an n-dimensional matrix representation of a group G. Define a G-action on the matrix ring $M_n(K)$ by:

$$(g, A) \mapsto \Phi(g) \cdot A \quad \text{(matrix multiplication)}$$

for $g \in G$ and $A \in M_n(K)$. This action induces a group homomorphism $\Psi\colon G \to \mathrm{GL}(M_n(K))$. Express the character χ_Ψ of Ψ in terms of χ_Φ (the character of Φ).

Problem 2.16 (S2015-Q5). Prove that a tensor product of irreducible representations over an algebraically closed field is irreducible.

Problem 2.17 (S2001-Q3). Calculate the complete character table for $\mathbb{Z}/3\mathbb{Z} \times S_3$, where S_3 is the symmetric group in 3 letters.

2.2 Induced representations

Problem 2.18 (S2009-Q6). Let $G = S_4$ and consider the subgroup $H = \langle (1\,2), (3\,4) \rangle$.

(a) Determine the number of irreducible complex characters of H.

(b) Choose a non-trivial irreducible character ψ of H over $\mathbb{C}$ satisfying $\psi((1\,2)(3\,4)) = -1$. Compute the values of the induced character $\mathrm{ind}_H^G(\psi)$ on all conjugacy classes of G, and express it as a sum of irreducible characters of G.

2.3 Frobenius Reciprocity

Problem 2.19 (S2017-Q6). Let G be a finite group and H an abelian subgroup. Show that every irreducible representation of G over $\mathbb{C}$ has dimension $\leq [G : H]$.

Proof. We know that if A is commutative, then all the irreducible representations ρ of A are one-dimensional. Now we induce ρ to a representation on G:

$$\bar{\rho} : G \to \mathrm{GL}(\mathbb{C})$$

We have

$$\mathrm{Ind}_A^G = \bigoplus_{i=1}^{n} g_i V$$

where g_i is the representative for each coset G/A, and $n = [G : A]$. Therefore all representations of G has dimension $[G : A]$. Since not all induced representataions are irreducible, any irreducible representation of G has dimension $\leq [G : A]$, as desired. $\square$

Problem 2.20 (S2008-Q6). Give an example of non-isomorphic finite groups with same character table. Construct the character table in detail.

Problem 2.21 (S2012-Q4). Let Q be the quaternion group with presentation:

$$Q = \langle t, s_i, s_j, s_k \mid t^2 = 1,\ s_i^2 = s_j^2 = s_k^2 = s_i s_j s_k = t \rangle.$$

(a) Find four non-isomorphic 1-dimensional real representations of Q.

(b) Prove that the natural embedding $\rho\colon Q \to \mathbb{H}$ given by:

$$\rho(t) = -1, \quad \rho(s_i) = i, \quad \rho(s_j) = j, \quad \rho(s_k) = k$$

defines an irreducible 4-dimensional real representation of Q, where $\mathbb{H}$ is the algebra of real quaternions.

(c) Classify all irreducible complex representations of Q up to isomorphism.

Problem 2.22 (F2004-Q6). Let D_8 be the dihedral group of order 8, with presentation:

$$D_8 = \langle r, s \mid r^4 = 1 = s^2,\ rs = sr^{-1} \rangle.$$

1. Determine all conjugacy classes of D_8.
2. Find the commutator subgroup D_8' of D_8 and determine the number of distinct degree-1 (linear) characters of D_8.
3. Construct the complete complex character table of D_8.

Problem 2.23 (F2000-Q7). Let D_{10} be the dihedral group of order 10, with presentation:

$$D_{10} = \langle r, s \mid r^5 = 1 = s^2,\ rs = sr^{-1} \rangle.$$

1. Determine all conjugacy classes of D_{10}.
2. Compute the commutator subgroup D_{10}' of D_{10}.
3. Prove that $D_{10}/D_{10}' \cong \mathbb{Z}/2\mathbb{Z}$ and deduce that D_{10} has exactly two distinct degree-1 characters.
4. Construct the complete complex character table of D_{10}.

Chapter 3

Semisimple Algebra

Page 19-20

The most recent semisimple question appeared in 2020.

Problem 3.1 (F2019-Q5). Determine the number of two-sided ideals in the group algebra $\mathbb{C}[S_3]$, where S_3 is the symmetric group of permutations of $\{1, 2, 3\}$.

Problem 3.2 (F2009-Q6, F2001-Q5). Let $\rho\colon G \to \mathrm{GL}_n(\mathbb{C})$ be an irreducible complex representation of a finite group G, with character χ, and let C be the center of G.

1. Prove that for every $s \in C$, the matrix $\rho(s)$ is a scalar multiple of the identity matrix I_n.
2. Using part (a), show that $|\chi(s)| = n$ for all $s \in C$.
3. Establish the inequality $n^2 \leq [G : C]$, where $[G : C]$ is the index of C in G.
4. Prove that if ρ is faithful (i.e., injective), then C must be cyclic.

Proof.

1. $\mathbb{C}$ is algebraically closed therefore Schur's lemma applies (see F2017-Q6)
2. We know that
$$\rho(z) = \begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & \lambda & \dots & 0 \\ \dots & & & \\ 0 & \dots & 0 & \lambda \end{pmatrix}$$
We also know that C is finite and $\rho(z^r) = I$, which implies $|r| = 1$. This gives $|\chi(s)| = n$ for all $s \in C$.
3. Y
4. If ρ is faithful, then C embeds into $k^\times$, and any finite subgroup of $k^\times$ is cyclic.

□

Problem 3.3 (S2017-Q5). Prove directly from the definition of (left) semisimple ring that every such ring is (left) Noetherian and Artinian. (You may freely use facts about semisimple, Noetherian, and Artinian modules.)

Problem 3.4 (S2005-Q4). Let R be a ring and L a minimal left ideal of R (i.e., L contains no non-zero proper left ideals of R). Assuming $L^2 \neq 0$, prove that $L = Re$ for some non-zero idempotent element $e \in R$.

Problem 3.5 (S2016-Q6, F2006-Q6, F2008-Q6). Let A be a finite-dimensional semisimple algebra over $\mathbb{C}$, and let V be an A-module that decomposes as $V \cong S \oplus S$, where S is a simple A-module. Determine the automorphism group $\mathrm{Aut}_A(V)$ of V as an A-module.

Problem 3.6 (S2010-Q5). Classify all non-commutative semi-simple rings with 512 elements. (You can use the fact that finite division rings are fields.)

Problem 3.7 (F2011-Q5). Let A be a finite-dimensional semisimple algebra over $\mathbb{C}$, and let V be a finitely-generated A-module. Prove that V has only finitely many A-submodules if and only if V decomposes into a direct sum of pairwise irreducible non-isomorphic (i.e., simple) A-modules.

Warning 3.1. For one-dimensional irreducible representation, $\rho : G \to \mathrm{GL}_n(\mathbb{C})$, they are equivalent to $\rho : G^{ab} \to \mathrm{GL}_n(\mathbb{C})$.

Chapter 4

Linear Algebra I

Topics: finitely generated modules/PID, triangularization, diagonalization, Jordan canonical form.
Page 21-23

Problem 4.1 (F2018-Q1). Let V be an n-dimensional vector space over a field k and let $\alpha : V \to V$ be a linear endomorphism. Prove that the minimal and characteristic polynomials of α coincide if and only if there is a vector $v \in V$ so that:

$$\{v, \alpha(v), \dots, \alpha^{n-1}(v)\}$$

is a basis for V.

Proof. We will show there is not vector $v \in V$ such that $\{v, \alpha(v), \dots, \alpha^{n-1}(v)\}$ is linearly independent if and only if the minimal and characteristic polynomials aren't the same.

$$\begin{aligned}\text{no } v \text{ s.t. } \{v, \dots, \alpha^{n-1}(v)\} \text{ is linearly independent} &\iff \text{for all } v \in V, \{v, \dots, \alpha^{n-1}v\} \text{is linearly dependent}\\ &\iff \alpha^{n-1}v = c_0 v + \cdots + c_{n-2}\alpha^{n-2}v \text{ for all } v\end{aligned}$$

We then claim that $\alpha^{n-1}v = c_0 v + \cdots + c_{n-2}\alpha^{n-2}v$ for all v if and only if the minimal polynomial p_m has degree less than the characteristic polynomial p_n. Note that p_n has degree n, and we can write

$$p_n(t) = a_n t^n + \cdots + a_1 t + a_0$$

and $p_n(\alpha)v = 0$ for all $v \in V$, therefore $\alpha^{n-1}v = c_0 v + \cdots + c_{n-2}\alpha^{n-2}v$ for all v if and only if

$$p_n(\alpha)v = a_n\alpha^{n-1}v + \cdots + a_1\alpha v + a_0 = p_{n-1}(\alpha)v = 0$$

where p_{n-1} is a polynomial of degree at most $n-1$ and is such that $p_{n-1}(\alpha) = 0$. Thus no v such that $\{v, \dots, \alpha^{n-v}v\}$ is linearly independent if and only if minimal and characteristic polynomial have different degrees. □

Problem 4.2 (F2018-Q3).

(a) Fix a positive integer n and classify all finite modules over the ring $\mathbb{Z}/n$.

(b) Prove, either using (a) or from first principles, for a fixed prime p that all finite modules over $\mathbb{Z}/p$ are free.

Problem 4.3 (F2017-Q2). Let Λ be a free abelian group of finite rank n, and let $\Lambda' \subset \Lambda$ be a subgroup of the same rank. Let $x_1, \dots, x_n$ be a $\mathbb{Z}$-basis for Λ, and let $x_1', \dots, x_n'$ be a $\mathbb{Z}$-basis for Λ'. For each i, write $x_i' = \sum_{j=1}^n a_{ij}x_j$, and let $A := (a_{ij}) \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$. Show that the index $[\Lambda : \Lambda']$ equals $|\det A|$.

Problem 4.4 (S2001-Q5).

(a) Prove that an $n \times n$ matrix A with entries in the field $\mathbb{C}$ of complex numbers, satisfying $A^3 = A$, can be diagonalized over $\mathbb{C}$.

(b) Does the statement in (a) remain true if one replaces $\mathbb{C}$ by an arbitrary algebraically closed field F? Why or why not?

Proof. (a) A is diagonalizable if and only if the minimal polynomial splits into distinct linear factors. The characteristic polynomial is $p(t) = t(t+1)(t-1)$ and the minimal polynomial $p_m \mid p$ thus A is diagonalizable.

(b) This is not true. Take k to be a field of characteristic 2, then

$$p(t) = t(t^2 - 1) = t(t-1)^2$$

Thus the minimal polynomial could be $(t-1)^2$, i.e., A is not necessarily diagonalizable.

$\square$

Problem 4.5 (F2001-Q3). Let A be an $n \times n$ complex matrix with $A^m = 0$ for some integer $m > 0$.

1. Show that if λ is an eigenvalue of A, then $\lambda = 0$.
2. Determine the characteristic polynomial of A.
3. Prove that $A^n = 0$.
4. Construct a 5×5 matrix B satisfying $B^3 = 0$ but $B^2 \neq 0$.
5. For any 5×5 complex matrix M with $M^3 = 0$ and $M^2 \neq 0$, is M necessarily similar to your matrix B from part (d)? Justify your answer.

1. Suppose λ is an eigenvalue, then there exists $v \neq 0$, such that

$$A^m v = \lambda^m v = 0 \Rightarrow \lambda = 0$$

2. The characteristic polynomial is $p(t) = t^n$.
3. Cayley-Hamilton theorem.
4. Can have

$$B = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The important is that the top left 3×3 matrix A satisfies $A^3 = 0, A^3 \neq 0$. This is constructed by building B using the Jordan form.

5. No, the lower 2×2 matrix could be

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Problem 4.6 (F2018-Q4). In this question all modules are left modules.

Let k be a field of characteristic different from 2 and let $G = \{e, g\}$ be the multiplicative group with two elements. Consider the group ring $A = k[G]$.

(a) Show that the A-module A is a direct sum of two ideals of A.

- List all proper ideals of A.
- Is A a principal ideal domain?

(b) Show that every A-module decomposes into a direct sum of simple A-modules.

(c) Assume now that the characteristic of k is 2. Give an example of an A-module that cannot be decomposed into a direct sum of two simple A-modules.

Problem 4.7 (S2003-Q3). Prove that if a linear operator on a complex vector space is diagonal in some basis, then its restriction to any invariant subspace L is also diagonal in some basis of L.

Proof. □

End of Page 22

Problem 4.8 (S2017-Q4). Let M be an invertible $n \times n$ matrix with entries in an algebraically closed field k of characteristic not 2. Show that M has a square root, i.e. there exists $N \in \mathrm{Mat}_{n\times n}(k)$ such that $N^2 = M$.

Problem 4.9 (S2008-Q1). Let k be a field. Consider the subgroup $B \subset \mathrm{GL}_2(k)$ where

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in k, ad \neq 0 \right\}.$$

(a) Let Z be the center of $\mathrm{GL}_2(k)$. Show that

$$\bigcap_{x \in \mathrm{GL}_2(k)} x^{-1} B x = Z.$$

(b) Assume k is algebraically closed. Show that

$$\bigcup_{x \in \mathrm{GL}_2(k)} x^{-1} B x = \mathrm{GL}_2(k).$$

(c) Assume k is a finite field. Can the statement in (b) still be true?

Proof. (a) Let $y \in \bigcap_{x \in \mathrm{GL}_2(k)}$, then for all $x \in \mathrm{GL}_2(k)$, we have $xyx^{-1} \in B$. This shows that

$$\begin{aligned}
xyx^{-1} \in B \text{ for all } x &\iff xyx^{-1}\begin{bmatrix} 0 \\ 1 \end{bmatrix} \in \left\langle \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\rangle \\
&\iff x^{-1}\begin{bmatrix} 0 \\ 1 \end{bmatrix} \text{ is a subspace for } y \text{ for all } x \\
&\iff \text{the whole vector space is the eigenspace of } y \\
&\iff y \text{ is a scalar} \\
&\iff y \in Z
\end{aligned}$$

(b) If k is algebraically closed, then any matrix can be written as a triangular matrix up to some basis change.

(c) (If k is R, the statement of (b) is also wrong). It's the same idea for finite groups, one can take $g \in \overline{\mathbb{F}_p} \backslash \mathbb{F}_p$, then the characteristic polynomial for the map of multiplication by $g : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ where $\overline{\mathbb{F}_p} = \mathbb{F}_{p^2}$ is a vector space over $\mathbb{F}$ the minimial polynomial is $(t-g)^2$ which is irreducible over $\mathbb{F}_p$.

□

Problem 4.10 (S2009-Q4)**.** Let E be a finite-dimensional vector space over an algebraically closed field k. Let A, B be k-endomorphisms of E. Assume $AB = BA$. Show that A and B have a common eigenvector.

Proof. Since k is algebraically closed, we know there exists at least one eigenvector of A, i.e., there exists λ such that $Av = \lambda v$ for some $v \neq 0$. We denote this eigenspace by E_λ, and we note that E_λ is invariant under B: let $v \in E_\lambda$

$$A(Bv) = \lambda(Bv)$$

thus $Bv \in E_\lambda$ as well. Then it suffices to find an eigenvector of B living inside E_λ, this is done by noting $B|_{E_\lambda}$ has an eigenvector in E_λ, as desired. □

Problem 4.11 (F2005-Q6)**.** Let E be a finite-dimensional vector space over a field k. Assume $S, T \in \mathrm{End}_k(E)$. Assume $ST = TS$ and both of them are diagonalizable. Show that there exists a basis of E consisting of eigenvectors for both S and T.

Proof. It is the same proof as above except now we do this for all $E_{\lambda_1}, \ldots, E_{\lambda_k}$. □

Problem 4.12 (S2015-Q2)**.** Let A, B be two commuting operators on a finite dimensional space V over $\mathbb{C}$ such that $A^n = B^m$ is the identity operator on V for some positive integers n, m. Prove that V is a direct sum of 1-dimensional invariant subspaces with respect to A and B simultaneously.

Proof. □

Chapter 5

Linear Algebra II

Topics: exterior power, tensor algebras, trances, determinants
Page 24-25

Problem 5.1 (F2016-Q5). Let A be a linear transformation of a finite dimensional vector space over a field of characteristic $\neq 2$.

(1) Define the wedge product linear transformation $\wedge^2 A = A \wedge A$.

(2) Prove that
$$tr(\wedge^2 A) = \frac{1}{2}(tr(A)^2 - tr(A^2)).$$

Problem 5.2 (S2006-Q5). Let V be a finite-dimensional vector space over a field k. Let $T \in \mathrm{End}_k(V)$. Show that $\mathrm{tr}(T \otimes T) = (\mathrm{tr}(T))^2$. Here $\mathrm{tr}(T)$ is the trace of T.

Problem 5.3 (S2016-Q4). Let V and W be two finite dimensional vector spaces over a field K. Show that for any $q > 0$,
$$\bigwedge^q (V \oplus W) \cong \sum_{i=0}^{q} (\bigwedge^i (V) \otimes_K \bigwedge^{q-i} (W)).$$

Problem 5.4 (S2011-Q4). Let F be a field, and V a finite-dimensional vector space over F, with $\dim_F V = n$.

(a) Prove that if $n > 2$, the spaces $\bigwedge^2(\bigwedge^2(V))$ and $\bigwedge^4(V)$ are not isomorphic.

(b) Let k be a positive integer. Prove that when $v \in \bigwedge^k(V)$ and $0 \neq x \in V$, $v \wedge x = 0$ holds if and only if $v = x \wedge y$ for some $y \in \bigwedge^{k-1}(V)$.

Problem 5.5 (S2010-Q4). Let V be a n-dimensional vector space over a field k. Let $T \in \mathrm{End}_k(V)$.

(a) Show that $tr(T \otimes T \otimes T) = (tr(T))^3$. Here $tr(T)$ is the trace of T.

(b) Find a similar formula for the determinant $\det(T \otimes T \otimes T)$.

Chapter 6

Linear Algebra III

Topics: random linear algebra problems

Page 26-28

Proposition 6.1. Let V be a m dimensional vector space, and W be n dimensional. Show that $A : V \to V$ and $B : W \to W$ has

$$\text{Tr}(A \otimes B) = \text{Tr}(A)\text{Tr}(B)$$

Problem 6.1 (S2013-Q5). Let A and B be $n \times n$ matrices with complex coefficients. Assume that $(A - I)^n = 0$ and $A^k B = BA^k$ for some natural number k. Prove that $AB = BA$ (*Hint*: Prove that A can be expressed as a function of A^k).

Problem 6.2 (F2011-Q2). Consider the special orthogonal group $G = SO(3, \mathbb{R})$, namely,

$$G = \{A \in GL(3, \mathbb{R}) : A^T A = \text{I}_3, \det(A) = 1\}$$

(a) Show that for any element A in G, there exists a real number α with $-1 \leq \alpha \leq 3$ such that

$$A^3 - \alpha A^2 + \alpha A - \text{I}_3 = 0.$$

(b) For which real numbers α with $-1 \leq \alpha \leq 3$ does there exist an element A in G whose minimal polynomial is $x^3 - \alpha x^2 + \alpha x - 1$? Explain your answer.

Problem 6.3 (F2007-Q3). Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a real matrix such that $a, b, c, d > 0$.

(1) Prove that A has two distinct real eigenvalues, $\lambda > \mu$.

(2) Prove that λ has an eigenvector in the first quadrant and μ has an eigenvector in the second quadrant.

Problem 6.4 (S2007-Q1). Prove that the integer orthogonal group $O_n(\mathbb{Z})$ is a finite group. (By definition, an $n \times n$ square matrix X over $\mathbb{Z}$ is orthogonal if $XX^t = I_n$.)

Problem 6.5 (F2008-Q4). A differentiation of a ring R is a mapping $D : R \to R$ such that, for all $x, y \in R$,

(1) $D(x + y) = D(x) + D(y)$; and

(2) $D(xy) = D(x)y + xD(y)$.

If K is a field and R is a K-algebra, then its differentiation are supposed to be over K, that is,

(3) $D(x) = 0$ for any $x \in K$.

Let D be a differentiation of the K-algebra $M_n(K)$ of $n \times n$-matrices. Prove that there exists a matrix $A \in M_n(K)$ such that $D(X) = AX - XA$ for all $X \in M_n(K)$.

Problem 6.6 (F2006-Q1). Let $\mathrm{SL}_n(k)$ be the special linear group over a field k, i.e, $n \times n$ matrices with determinant 1. Let I be the identity matrix, and E_{ij} be the elementary matrix that has 1 at (i, j)-entry and 0 elsewhere. Here $1 \leq i \neq j \leq n$.

(1) Let C_{ij} be the centralizer of the matrix $I + E_{ij}$. Find explicit generators of C_{ij}.

(2) Find the intersection

$$\bigcap_{1 \leq i \neq j \leq n} C_{ij}.$$

(3) Determine all the elements in the conjugacy class of $I + E_{ij}$.

Problem 6.7 (S2018-Q1). Let F be a field of characteristic not equal to 2. Let D be the non-commutative algebra over F generated by elements i, j that satisfy the relations

$$i^2 = j^2 = 1, \quad ij = -ji.$$

Define $k = ij$.

(a) Verify that D is isomorphic to the algebra $M_2(F)$ of 2×2 matrices in such a way that

$$1 \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, j \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, k \leftrightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(b) Write $q = x + yi + zj + uk$ for $x, y, z, u \in F$. Verify that the norm

$$N(q) = x^2 - y^2 - z^2 + u^2$$

corresponds to the determinant under the isomorphism of part (a).

(c) What does the involution $q \mapsto \bar{q} = x - yi - zj - uk$ on D correspond to on the matrix side?

Problem 6.8 (S2006-Q3). Let V be a n-dimensional vector space over a field k, with a basis $\{e_1, \ldots, e_n\}$. Let A be the ring of all $n \times n$ diagonal matrices over k. V is a A-module under the action:

$$\mathrm{diag}(\lambda_1, \ldots, \lambda_n) \cdot (a_1 e_1 + \cdots + a_n e_n) = (\lambda_1 a_1 e_1 + \cdots + \lambda_n a_n e_n).$$

Find all A-submodules of V.

Problem 6.9 (S2006-Q1). Let $\mathbb{F}_p$ be the field with p elements, here p is prime. Let $\mathrm{SL}_2(\mathbb{F}_p)$ be the group of 2×2 matrices over $\mathbb{F}_p$ with determinant 1.

(1) Find the order of $\mathrm{SL}_2(\mathbb{F}_p)$. Deduce that

$$H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_p \right\}$$

is a Sylow-subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$.

(2) Determine the normalizer of H in $\mathrm{SL}_2(\mathbb{F}_p)$ and find its order.

Problem 6.10 (S2004-Q1). Let $\mathbb{F}_2$ be the finite field with 2 elements.

(a) What is the order of $\mathrm{GL}_3(\mathbb{F}_2)$, the group of 3×3 invertible matrices over $\mathbb{F}_2$?

(b) Assuming the fact that $\mathrm{GL}_3(\mathbb{F}_2)$ is a simple group, find the number of elements of order 7 in $\mathrm{GL}_3(\mathbb{F}_2)$.

Problem 6.11 (S2002-Q4). For a field K, let $\mathrm{SL}_2(K)$ be the special linear group over K, i.e. the group of 2×2-matrices over K with determinant 1, and let $\mathrm{PSL}_2(K)$ be the quotient of $\mathrm{SL}_2(K)$ by its center, i.e. the projective special linear group. Find the order of $\mathrm{PSL}_2(F_7)$ where F_7 denotes the finite field of 7 elements.

Problem 6.12 (S2007-Q4). Find the invertible elements, the zero divisors and the nilpotent elements in the following rings:

(a) $\mathbb{Z}/p^n\mathbb{Z}$, where n is a natural number, p is a prime one.

(b) the upper triangular matrices over a field.

Chapter 7

Homological Algebra

Page 29-34

Problem 7.1 (S2012-Q2).

(a) Prove that if M is an abelian group and n is a positive integer, the tensor product $M \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ can be naturally identified with M/nM.

(b) Compute the tensor product over $\mathbb{Z}$ of $\mathbb{Z}/n\mathbb{Z}$ with each of $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$. Also compute the tensor products $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$, $\mathbb{Q} \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})$, and $(\mathbb{Q}/\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})$.

(c) Let $\mathbb{Z}^{\mathbb{N}}$ denote the (abelian) group of sequences $(a_i)_{i\in\mathbb{N}}$ in $\mathbb{Z}$ under termwise addition, and $\mathbb{Z}^{(\mathbb{N})}$ the subgroup of sequences for which $a_i = 0$ for all but finitely many i. Define $\mathbb{Q}^{\mathbb{N}}$ and $\mathbb{Q}^{(\mathbb{N})}$ analogously. Compare $\mathbb{Z}^{(\mathbb{N})} \otimes_{\mathbb{Z}} \mathbb{Q}$ to $\mathbb{Q}^{(\mathbb{N})}$, and $\mathbb{Z}^{\mathbb{N}} \otimes_{\mathbb{Z}} \mathbb{Q}$ to $\mathbb{Q}^{\mathbb{N}}$.

Problem 7.2 (F2006-Q4). Let R be a commutative ring. Let M be an R-module.

(1) Write down the definition of $\mathcal{T}(M)$, the tensor algebra of M.

(2) Assume $R = \mathbb{Z}$ and $M = \mathbb{Q}/\mathbb{Z}$. Compute $\mathcal{T}(M)$.

(3) If M is a vector space over a field R, show that $\mathcal{T}(M)$ contains no zero divisors.

Problem 7.3 (S2009-Q5). Consider the $\mathbb{Z}$-modules $M_i = \mathbb{Z}/2^i\mathbb{Z}$ for all positive integers i. Let $M = \prod_{i=1}^{\infty} M_i$. Let $S = \mathbb{Z} - \{0\}$.

(a) Show that
$$\mathbb{Q} \otimes_{\mathbb{Z}} M \cong S^{-1}M.$$
Here $S^{-1}M$ is the localization of M.

(b) Show that
$$\mathbb{Q} \otimes_{\mathbb{Z}} \prod_{i=1}^{\infty} M_i \neq \prod_{i=1}^{\infty} (\mathbb{Q} \otimes_{\mathbb{Z}} M_i).$$

Problem 7.4 (S2013-Q1). Prove that, as a $\mathbb{Z}$-module, $\mathbb{Q}$ is flat but not projective.

Problem 7.5 (F2008-Q5). For each $n \in \mathbb{Z}$, define the ring homomorphism

$$\phi_n : \mathbb{Z}[x] \to \mathbb{Z} \text{ by } \phi_n(f) = f(n).$$

This gives a $\mathbb{Z}[x]$-module structure on $\mathbb{Z}$, i.e,

$$f \circ a = f(n) \cdot a \text{ for all } f \in \mathbb{Z}[x] \text{ and } a \in \mathbb{Z}.$$

Now given two integers $m, n \in \mathbb{Z}$, compute the tensor product $\mathbb{Z} \otimes_{\mathbb{Z}[x]} \mathbb{Z}$ where the left-hand copy of $\mathbb{Z}$ uses the module structure from ϕ_n and the right-hand copy of $\mathbb{Z}$ uses the module structure from ϕ_m. (Note: The answer depends on the numbers n and m.)

Problem 7.6 (F2014-Q2). Let $R = \mathbb{Q}[X]$, I and J the principal ideals generated by $X^2 - 1$ and $X^3 - 1$ respectively. Let $M = R/I$ and $N = R/J$. Express in simplest terms [the isomorphism type of] the R-modules $M \otimes_R N$ and $\mathrm{Hom}_R(M, N)$. **Explain.**

Problem 7.7 (F2004-Q5). Consider the ideal $I = (2, x)$ in $R = \mathbb{Z}[x]$.

(a) Construct a non-trivial R-module homomorphism $I \otimes_R I \to R/I$, and use that to show that $2 \otimes x - x \otimes 2$ is a non-zero element in $I \otimes_R I$.

(b) Determine the annihilator of $2 \otimes x - x \otimes 2$.

Problem 7.8 (S2018-Q5). Let n be a positive integer and A an abelian group. Prove that

$$\mathrm{Ext}^1(\mathbb{Z}/n\mathbb{Z}, A) \cong A/nA.$$

Problem 7.9 (F2002-Q3). Working over the integers, calculate (and show your work in a readable fashion) $\mathrm{Tor}(\mathbb{Z}/(p), \mathbb{Z}/(p))$.

Problem 7.10 (F2002-Q4). Working over the integers, calculate (and show your work in a readable fashion) $\mathrm{Ext}(\mathbb{Z}/(p), \mathbb{Z}/(p))$.

Problem 7.11 (S2018-Q2). Let R be a commutative ring. An R-module M is said to be finitely presented if there exists a right-exact sequence

$$R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

for some non-negative integers m, n. Prove that any finitely generated projective R-module P is finitely presented.

Problem 7.12 (F2013-Q3)**.** Let R be a commutative ring with unity. Given an R-module A and an ideal $I \subset R$, there is a natural R-module homomorphism $A \otimes_R I \to A \otimes_R R \cong A$ induced by the inclusion $I \subset R$. In the following three steps you shall prove the flatness criterion: *A is flat if and only if for every finitely generated ideal $I \subset R$ the natural map $A \otimes_R I \to A \otimes_R R$ is injective.*

(a) Prove that if A is flat and $I \subset R$ is a finitely generated ideal then $A \otimes_R I \to A \otimes_R R$ is injective.

(b) If $A \otimes_R I \to A \otimes_R R$ is injective for every finitely generated ideal I, prove that $A \otimes_R I \to A \otimes_R R$ is injective for every ideal I. Show that if K is any submodule of a free module F then the natural map $A \otimes_R K \to A \otimes_R F \cong A$ induced by the inclusion $K \subset F$ is injective (*Hint*: the general case reduces to the case when F has finite rank).

(c) Let $\psi : L \to M$ be an injective homomorphism of R-modules. Prove that the induced map $1 \otimes \psi : A \otimes_R L \to A \otimes_R M$ is injective (*Hint*: Write M as a quotient $f : F \to M$ of a free module F, giving a short exact sequence $0 \to K \to F \to M \to 0$ and consider the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r] \arrow[d, "\mathrm{id}"] & J \arrow[r] & L \arrow[r] \arrow[d, "\varphi"] & 0 \\
0 \arrow[r] & K \arrow[r] & F \arrow[r, "f"] & M \arrow[r] & 0
\end{tikzcd}$$

where $J = f^{-1}(\psi(L))$).

Problem 7.13 (F2013-Q4)**.**

(a) Let R be a P.I.D. Prove that a finitely generated R-module M is flat if and only if M is torsion-free (hence, free by the structure theorem).

(b) Give an example of an integral domain R and a torsion-free R-module M such that M is not free.

Problem 7.14 (F2000-Q6)**.** Let R be the ring $\mathbb{Q}[X]/(X^7 - 1)$, where $(X^7 - 1)$ is the ideal generated by $X^7 - 1$ in $\mathbb{Q}[X]$. Give an example of a finitely generated projective R-module which is not R-free. (We remind you that an R-module is called projective if it is a direct summand of a free R-module.)

Chapter 8

Commutative Algebra

Topics: basic properties, Nakayama's lemma, integrality.
Page 35-40

Problem 8.1 (S2017-Q1). Let A be a commutative ring, and define the *nilradical* $\sqrt{0}$ to be the set of nilpotent elements in A. Show that $\sqrt{0}$ is equal to the intersection of all prime ideals in A. Show that if A is reduced, then A can be embedded into a product of fields.

This one is complicated manipulation, so we omit.

Problem 8.2 (F2004-Q2). Let $\mathfrak{N}$ be the set of all nilpotent elements in a ring R. Assume first that R is commutative.

(a) Show that $\mathfrak{N}$ is an ideal in R, and $R/\mathfrak{N}$ contains no non-zero nilpotent elements.

(b) Show that $\mathfrak{N}$ is the intersection of all the prime ideals of R.

(c) Give an example with R **non**-commutative where $\mathfrak{N}$ is not an ideal in R.

Problem 8.3 (S2014-Q4). Let L/K be a Galois extension of degree p with $\mathrm{char} K = p$. Show that $L = K(\theta)$, where θ is a root of $x^p - x - a, a \in K$, and, conversely, any such extension is Galois of degree 1 or p.

Problem 8.4 (S2009-Q2). Consider $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ where ω is a non-trivial cube root of 1. Show that $\mathbb{Z}[\omega]$ is an Euclidean domain.

Problem 8.5 (F2006-Q3). Let A be a principal integral domain and K be its field of fractions. Assume that R is a ring such that $A \subset R \subset K$. Show that R is also a principal integral domain.

Problem 8.6 (F2001-Q2). Let S denote the ring $\mathbb{Z}[X]/X^2\mathbb{Z}[X]$, where X is a variable.

(a) Show that S is a free $\mathbb{Z}$-module and find a $\mathbb{Z}$-basis for S.

(b) Which elements of S are units (i.e. invertible with respect to multiplication)?

(c) List all the ideals of S.

(d) Find all the nontrivial ring morphisms defined on S and taking values in the ring of Gaussian integers $\mathbb{Z}[i]$.

Problem 8.7 (S2001-Q6). Let R be the ring $\mathbb{Z}[X,Y]/(YX^2 - Y)$, where X and Y are two algebraically independent variables, and $(YX^2 - Y)$ is the ideal generated by $YX^2 - Y$ in $\mathbb{Z}[X,Y]$.

(a) Show that the ideal I generated by $Y - 4$ in R is not prime.

(b) Provide the complete list of prime ideals in R containing the ideal I described in question (a).

(c) Which of the ideals found in (b) are maximal?

Problem 8.8 (F2017-Q3). In this problem all rings are commutative.

(a) Let R be a local ring with maximal ideal $\mathfrak{m}$, let N and M be finitely generated R-modules, and let $f\colon N \to M$ be an R-linear map. Show that f is surjective if and only if the induced map $N/\mathfrak{m}N \to M/\mathfrak{m}M$ is.

(b) Recall that a module M over a ring R is *projective* if the functor $\mathrm{Hom}_R(M, -)$ is exact. Show that if R is local and M is finitely generated projective, then M is free.

Problem 8.9 (F2010-Q4). Let A be a commutative Noetherian local ring with maximal ideal $\mathfrak{m}$. Assume $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for some $n > 0$. Show that A is Artinian.

Problem 8.10 (F2009-Q5). Let A, B be two Noetherian local rings with maxima ideals m_A, m_B, respectively. Let $f : A \to B$ be a ring homomorphism such that $f^{-1}(m_B) = m_A$. Assume that:

1. $A/m_A \to B/m_B$ is an isomorphism.
2. $m_A \to m_B/m_B^2$ is surjective.
3. B is a finitely generated A-module (via f). Show that f is surjective.

Problem 8.11 (F2015-Q6). Let K be a finite algebraic extension of $\mathbb{Q}$.

(a) Give the definition of an integral element of K.

(b) Show that the set of integral elements in K form a sub-ring of K.

(c) Determine the ring of integers in each of the following two fields No credit for memorized answers: $\mathbb{Q}(\sqrt{13})$, and $\mathbb{Q}(\sqrt[3]{2})$.

Problem 8.12 (F2009-Q2). Consider $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} | a, b \in \mathbb{Q}\}$. Determine the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{5}]$.

Problem 8.13 (S2012-Q5).

(a) Give the definition of a Dedekind domain.

(b) Give an example of a Dedekind domain that is not a principal ideal domain. Verify from the definition that it *is* a Dedekind domain, and also that it isn't a principal ideal domain.

Problem 8.14 (S2005-Q5). Let A be an integral domain and let K be its field of fractions. Let A' be the integral closure of A in K. Let $P \subset A$ be a prime ideal and let $S = A - P$. (Note that $A_P = S^{-1}A$ is contained in K.) Show that A_P is integrally closed in K if and only if $(A'A) \otimes_A A_P = 0$.

Problem 8.15 (F2013-Q2). Let a be an integral algebraic number such that its norm is 1 for any imbedding into $\mathbb{C}$, the field of complex numbers. Prove that a is a root of unity.

Problem 8.16 (F2004-Q4). Let $\lambda_1, \ldots, \lambda_n$ be roots of unity, with $n \geq 2$. Assume that $\frac{1}{n}\sum_{i=1}^{n} \lambda_i$ is integral over $\mathbb{Z}$. Show that either $\sum_{i=1}^{n} \lambda_i = 0$ or $\lambda_1 = \lambda_2 = \cdots = \lambda_n$.

Chapter 9

Ring Theory Random

Page 41

Proposition 9.1. Let $I \subset R$ be an ideal, then the following are equivalent:

1. I is a prime ideal.
2. There exists a field K and $\varphi : A \to K$ such that $I = \ker(\varphi)$.

Proof. (1)⇒(2). □

Problem 9.1 (S2010-Q2). Let R be a ring such that $r^3 = r$ for all $r \in R$. Show that R is commutative. (Hint: First show that r^2 is central for all $r \in R$.)

Proof. This question is not so constructive and is purely computational (as far as I am aware) so I will skip it here. □

Problem 9.2 (S2006-Q2). Let R be a ring with identity 1. Let $x, y \in R$ such that $xy = 1$.

(1) Assume R has no zero-divisor. Show that $yx = 1$.

(2) Assume R is finite. Show that $yx = 1$.

Proof. (1) We know $x, y \neq 0$, therefore consider

$$x(yx - 1) = 0$$

Since R has no zero-divisor, we must have $yx - 1 = 0$, as desired.

(2) We note the right multiplication map $m_x : R \to R$ by x is injective: suppose $r_1, r_2 \in R$ and

$$r_1 x = x r_2 x$$

multiplying both sides by y we see $r_1 = r_2$. Since R is finite, this map is also surjective, i.e., there exists $s \in R$ such that

$$sx = 1$$

Now we see

$$yx - 1 = sx(yx - 1) = sx - sx = 0$$

as desired.

□

Chapter 10

Tensor Products over Fields

Page 42-43

Proposition 10.1. If L/k is finite separate extension, then there exists $\alpha \in L$ such that

$$L = k(\alpha)$$

Example 10.1. Write $\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{3})$ as a product of fields:

$$\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \frac{\mathbb{Q}[x]}{(x^2-3)} \cong \frac{\mathbb{Q}(\sqrt{2}[x])}{(x^3-2)}$$

and (x^3-2) does not have a root in $\mathbb{Q}(\sqrt{2})$, thus

$$\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}) \cong \mathbb{Q}(\sqrt{2})\sqrt{3}$$

Example 10.2. Similarly, write the following as a product of fields

$$\begin{aligned}
\mathbb{Q}(\sqrt[4]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[4]{2}) &= \mathbb{Q}(\sqrt[4]{2}) \otimes_{Q} \frac{\mathbb{Q}[x]}{(x^4-2)} \\
&= \frac{\mathbb{Q}(\sqrt[4]{2})[x]}{(x^4-2)} \\
&= \frac{\mathbb{Q}(\sqrt[4]{2})[x]}{(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x^2+\sqrt{2})} \\
&= \frac{\mathbb{Q}(\sqrt[4]{2})[x]}{(x-\sqrt[4]{2})} \times \frac{\mathbb{Q}(\sqrt[4]{2})[x]}{(x+\sqrt[4]{2})} \times \frac{\mathbb{Q}(\sqrt[4]{2})[x]}{(x^2+\sqrt{2})}
\end{aligned}$$

By the Chinese Remainder theorem

Lemma 10.1 (CRT). Let R be a PID, and $I + J = (1)$, then

$$\frac{R}{IJ} = \frac{R}{I} \times \frac{R}{J}$$

We have

$$\mathbb{Q}(\sqrt[4]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}(\sqrt[4]{2}) \times \mathbb{Q}(\sqrt[4]{2}) \times \mathbb{Q}(\sqrt[4]{2})(i)$$

Example 10.3. The field extension generated $(x^p - t)$ of field $\mathbb{F}_p(t)$ is not separable, i.e.,

$$\frac{\mathbb{F}_p(t)[x]}{(x^p - t)}$$

is not separable. Consider the element x, then the minimal polynomial $m(s) = s^p - t$ can be written as

$$s^p - t = s^p - x^p = (s - x)^p$$

Problem 10.1 (S2017-Q3). Let K/k be a finite separable field extension, and let L/k be any field extension. Show that $K \otimes_k L$ is a product of fields.

Problem 10.2 (F2019-Q3). Let F, L be extensions of a field K. Suppose that F/K is finite. Show that there exists an extension E/K such that there are monomorphisms of F into E and of L into E which are identical on K.

Problem 10.3 (F2009-Q4). Let E and F be finite field extensions of a field k such that $E \cap F = k$, and that E and F are both contained in a larger field L. Assume that E is Galois over k. Show that $E \otimes_k F \cong EF$.

Problem 10.4 (S2008-Q5). Let k be a field of characteristic zero. Assume that E and F are algebraic extensions of k and both contained in a larger field L. Show that the k-algebra $E \otimes_k F$ has no nonzero nilpotent elements.

Problem 10.5 (S2004-Q5). Show that there is a $\mathbb{C}$-algebra isomorphism between $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ and $\mathbb{C} \times \mathbb{C}$.

Problem 10.6 (F2005-Q5). Let $\mathbb{C}$ and $\mathbb{R}$ be complex and real number fields. Let $\mathbb{C}(x)$ and $\mathbb{C}(y)$ be function fields of one variable. Consider $\mathbb{C}(x) \otimes_{\mathbb{R}} \mathbb{C}(y)$ and $\mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y)$.

(1) Determine if they are integral domains.

(2) Determine if they are fields.

Problem 10.7 (F2003-Q4). Verify the isomorphism of algebras over a field K:

$$\mathbb{M}_n(K) \otimes_K \mathbb{M}_m(K) \simeq \mathbb{M}_{mn}(K).$$

[Note: $\mathbb{M}_n(K)$ denotes the algebra of $n \times n$ matrices over K.]

Chapter 11

Irreducibility of Polynomials

Page 44-45

Proposition 11.1. Fix any prime p, the polynomial

$$f(x) = x^{p-1} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$. Similarly

$$g(x) = x^{p-1} - x^{p-2} + \cdots - x + 1$$

is irreducible over $\mathbb{Q}$.

Proof. This is an application of Eisenstein. Write

$$f(x) = \frac{x^p - 1}{x - 1}$$

and replace x with $x + 1$ we get

$$\begin{aligned} f(x) &= \frac{(x+1)^p - 1}{x} \\ &= \frac{\sum_{k=1}^{n} \binom{p}{k} x^k}{x} \\ &= \sum_{k=1}^{n} \binom{p}{k} x^{k-1} \end{aligned}$$

We apply Eisenstein with prime p to see f is irreducible. □

Proposition 11.2. For any prime p, either $\sqrt{2} \in \mathbb{F}_p$ or $\sqrt{3} \in \mathbb{F}_p$ or $\sqrt{6} \in \mathbb{F}_p$.

Proof. We know there exists a legendre symbol (a character) $\chi : \mathbb{F}_p^\times \to \{\pm 1\}$ such that for $g \in \mathbb{F}_p$,

$$\chi(g) = \begin{cases} 1, & \text{if } g \text{ is a square} \\ -1, & \text{if } g \text{ is not a square} \end{cases}$$

Suppose that $\sqrt{2}$ and $\sqrt{3}$ are not in $\mathbb{F}_p$, then

$$\chi(2) = \chi(3) = -1$$

i.e., $2, 3$ are not squares. However,

$$\chi(2 \cdot 3) = \chi(6) = 1$$

This implies that 6 is a square and $\sqrt{6} \in \mathbb{F}_p$, as desired. □

Corollary 11.1. The following polynomial

$$f(x) = (x^2 - 1)(x^3 - 1)(x^6 - 1)$$

has a linear factor.

Problem 11.1 (S2018-Q3). Let R be the ring $\mathbb{Z}[\zeta_p]$, where p is a prime number and ζ_p denotes a primitive pth root of unity in $\mathbb{C}$. Prove that if an integer $n \in \mathbb{Z}$ is divisible by $1 - \zeta_p$ in R, then p divides n.

Problem 11.2 (F2008-Q2). Show that the polynomial $x^5 - 5x^4 - 6x - 2$ is irreducible in $\mathbb{Q}[x]$.

Problem 11.3 (F2003-Q3). Obtain a factorization into irreducible factors in $\mathbb{Z}[x]$ of the polynomial $x^{10} - 1$.

Problem 11.4 (S2004-Q3). Let k be a field with characteristic 0. Let $m \geq 2$ be an integer. Show that $f(x, y) = x^m + y^m + 1$ is irreducible in $k[x, y]$.

Problem 11.5 (S2017-Q2, S2007-Q3). Write down the minimal polynomial for $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$ and prove that it is reducible over $\mathbb{F}_p$ for every prime number p.

Proof. The minimal polynomial of $\sqrt{2} + \sqrt{3}$ is

$$f(x) = x^4 - 10x^2 + 1 = 0$$

By the corollary, we know in any $\mathbb{F}_p$ for any prime p, either $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ is in $\mathbb{F}_p$. We claim that if $\sqrt{2} \in \mathbb{F}_p$, then f is factors over $\mathbb{Q}(\sqrt{2})$. Suppose that f does not factor over $\mathbb{Q}(\sqrt{2})$, i.e., f is irreducible over $\mathbb{Q}(\sqrt{2})$, then the degree of extension

$$[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 8$$

which is a contradiction. Hence f factors over $\mathbb{Q}(\sqrt{2})$. Similar arguments work if $\sqrt{3}$ or $\sqrt{6}$ are in $\mathbb{F}_p$. □

Problem 11.6 (S2015-Q4). Prove that the polynomial $x^4 + 1$ is not irreducible over any field of positive characteristic.

Proof. The idea is the same as above, and it suffices to note that the field extension generated by $x^4 + 1$ is $\mathbb{Q}(\sqrt{2}, i)$. Using the Legendre symbol, the proof is similar to the above. □

Problem 11.7 (F2010-Q2).

(a) Find the complete factorization of the polynomial $f(x) = x^6 - 17x^4 + 80x^2 - 100$ in $\mathbb{Z}[x]$.

(b) For which prime numbers p does $f(x)$ have a root in $\mathbb{Z}/p\mathbb{Z}$ (i.e, $f(x)$ has a root modulo p)? Explain your answer.

Proof. (a) Letting $y = x^2$, we need to factorize

$$f(y) = y^3 - 17y + 80y - 100$$

Now f is cubic, we need to find the roots of f: 5 is a root,

$$f(y) = (y-5)(y-2)(y-10)$$

i.e.,

$$f(x) = (x^2-2)(x^2-5)(x^2-10)$$

which consists of only irreducible factors over $\mathbb{Z}$.

(b) f has a root in $\mathbb{F}_p$ for all prime p, by the above corollary.

□

11.1 Quick finite field review

If p is prime, then $\mathbb{F}_p$ is a field of p elements, isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Proposition 11.3 (Fact)**.** For every prime power p^n, there is exactly one finite field of p^n elements, namely $\mathbb{F}_{p^n}$, up to isomorphisms.

Theorem 11.1 (Galois theory of finite fields)**.** We have

(1) $\mathbb{F}_{p^n}/\mathbb{F}$ is a Galois extension, and

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}) \text{ is cyclic}$$

where the generator is the Forbenius automorphism $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ where

$$\sigma : x \mapsto x^p$$

(2) We also have

$$\mathbb{F}_{p^n} = \left\{\alpha \in \overline{\mathbb{F}}_p : \alpha^{p^n} - \alpha = 0\right\}$$

This statement implies that $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - 1$.

Proof. We note that $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

$$\mathbb{F}_{p^n} = \left\{\alpha \in \overline{\mathbb{F}}_p : \alpha^{p^n} - \alpha = 0\right\}$$

If $\alpha \in \mathbb{F}_{p^n}$, then we want to show that $\alpha^{p^n} = \alpha$: if $\alpha = 0$, then done; if $\alpha \in \mathbb{F}_p^\times$, then using the fact that any finite field is cyclic, we know

$$\mathbb{F}_{p^n} \cong \mathbb{Z}/(p^n-1)\mathbb{Z} \Rightarrow \alpha^{p^n-1} = 1$$

and we are done. Now we observe that $\left\{\alpha \in \overline{\mathbb{F}}_p : \alpha^{p^n} - \alpha = 0\right\}$ has p^n elements, and is also a field, thus we are done.

This fact can be used to show (1) and the above proposition. □

Proposition 11.4. $\mathbb{F}_{p^n}$ embeds into $\mathbb{F}_{p^m}$ iff $n \mid m$.

Proof. If $n \mid m$, then $m = nk$ for some integer k. We then notice that

$$\alpha^{p^n} = \alpha \Rightarrow \alpha^{p^{kn}} = \alpha^{p^m} = \alpha$$

Thus $\mathbb{F}_{p^n}$ embeds into $\mathbb{F}_{p^m}$. Conversely, consider the Galois field extensions

$$\mathbb{F}_p \subset \mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$$

Then by degree of field extensions, we know $n \mid m$. □

Problem 11.8 (F2016-Q3)**.** If field $|F| = 2^n$, find all n such that $x^2 - x + 1$ is irreducible over F.

Proof. We know that $x^2 - x + 1$ is irreducible over $\mathbb{F}_2$, namely, it has no roots in $\mathbb{F}_2$. Since there is only one field of order 4, we must have

$$\mathbb{F}_4 \cong \frac{\mathbb{F}_2}{(x^2 - x + 1)}$$

Clearly $x^2 - x + 1$ is not irreducible over $\mathbb{F}_4$. For any $\mathbb{F}_{2^n}$, we know $(x^2 - x + 1)$ is irreducible if and only if $\mathbb{F}_4$ does not embed into $\mathbb{F}2^n$, i.e., $2 \nmid n$. This shows that when n is odd, the polynomial $x^2 - x + 1$ is irreducible over $\mathbb{F}_{2^n}$. □

Chapter 12

Galois Theory

Page 46 Page 52-61

Quick reminder whether a polynomial has a rational root:

Proposition 12.1. Let $f(t) = a_n t^n + \cdots + a_1 t + a_0$, and if a rational (expressed in lowest terms) $\frac{p}{q}$ is a root of f, then $p \mid a_0, q \mid a_0$.

Definition 12.1 (Galois extension). A field extension $k \subset L$ is Galois if for all $x \in L$, the minimal polynomial $f(x) \in k[x]$ splits into a linear factor without repeated roots.

Definition 12.2 (normal extension). An extension $k \subset K$ is normal if f has a root in K if and only if f splits completely into linear factors over K. An extension that is normal and separable is Galois.

Theorem 12.1. Suppose $k \subset L$ is Galois,

$$\{k \subset M \subset L\} \xLeftrightarrow{\text{one-to-one}} \{\text{Subgroups of } \mathrm{Gal}(L/k)\}$$

Moreover, the order of the Galois group is the degree of the field extension.

$$|\mathrm{Gal}(L/k)| = [L : k]$$

Proposition 12.2. Let G be a Galois group of a polynomial f of degree 4, and $|G| = 8$, then

$$G \cong D_8$$

Proof. We know that G permutes the four roots of f, i.e., G embeds into S_4. Since $|G| = 8$, we know G is a Sylow-2 subgroup of S_4, and all Sylow-2 subgroups are conjugates (isomorphic to one another), i.e.,

$$G \cong D_8$$

as desired. □

Proposition 12.3. Let $k \subset K$ be a Galois extension, then the intermediate field extensions $k \subset E \subset K$ is determined by the subgroups of $\mathrm{Gal}(K/k)$. Namely, let E be an intermediate extension, there exists a subgroup H of $\mathrm{Gal}(K/k)$ that fixes E. This extension is normal if and only if H is normal. And E/k is Galois if and only if H is normal.

Proposition 12.4. We can draw the lattice of subgroups of $\mathrm{Gal}(K/k)$ and lattice of subfields:

$$\begin{tikzcd}
k \arrow[r, dash, "\subseteq"] \arrow[d, dash, dashed] & E \arrow[r, dash, "\subseteq"] \arrow[d, dash, dashed] & F \arrow[d, dash, dashed] \\
\mathrm{Aut}_k(F) \arrow[r, dash, "\supseteq"'] & \mathrm{Aut}_E(F) \arrow[r, dash, "\supseteq"'] & \{e\}
\end{tikzcd}$$

Problem 12.1 (S2009-Q3)**.** Consider the field $K = \mathbb{Q}(\sqrt{a})$ where $a \in \mathbb{Z}, a < 0$. Show that K cannot be embedded in a cyclic extension whose degree over $\mathbb{Q}$ is divisible by 4.

Proof. Suppose K embedes into a degree $4n$ extension L, and

$$\mathrm{Gal}(L/\mathbb{Q}) = \frac{\mathbb{Z}}{4n\mathbb{Z}}$$

Since K is a degree 2 extension of $\mathbb{Q}$, thus L/K is a degree $4n/2$ Galois extension, with Galois group

$$\mathrm{Gal}(L/K) = \frac{2\mathbb{Z}}{4n\mathbb{Z}}$$

We notice that $\sqrt{a}$ is complex, hence the complex conjugation τ is in $\mathrm{Gal}(L/\mathbb{Q})$, i.e., it is an order 2 element in $\frac{\mathbb{Z}}{4n\mathbb{Z}}$, it is therefore $[2n]$ i.e.,

$$\tau \in \frac{2\mathbb{Z}}{4n\mathbb{Z}} = \mathrm{Gal}(L/\mathbb{Q})$$

This implies τ fixed K, however $\tau(\sqrt{a}) \neq \sqrt{a}$, hence a contradiction. □

Problem 12.2 (F2000-Q4)**.** Let G be a finite group. Show that there exists a Galois field extension K/k whose Galois group is isomorphic to G.

Problem 12.3 (S2001-Q2)**.** Let K be the splitting field of $f(X) = X^3 - 2$ over $\mathbb{Q}$.

(a) Determine an explicit set of generators for K over $\mathbb{Q}$.

(b) Show that the Galois group $G(K/\mathbb{Q})$ of K over $\mathbb{Q}$ is isomorphic to the symmetric group S_3.

(c) Provide the complete list of intermediate fields k, $\mathbb{Q} \subseteq k \subseteq K$, satisfying $[k : \mathbb{Q}] = 3$.

(d) Which of the fields determined in (c) are normal extensions of $\mathbb{Q}$?

Proof. (a) The set of generators is

$$\left\{\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right\}$$

(b) The minimal polynomial of $e^{\frac{2\pi i}{3}}$ is $x^2 + x + 1$. This shows that the Galois group G has order 6, and because of the complex root, there exists an element of order 2, a transposition, that only swaps the two complex roots, and G also has an element of order 3 because 3 divides $|G|$, this shows that G must be S_3.

(c) The following is the subgroup lattice of S_3 and subfield lattice:

$$\begin{tikzcd}
& K \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] \arrow[drr, dash, "3"] & & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash, "3"'] & \mathbb{Q}(\sqrt[3]{2}\omega) \arrow[d, dash, "3"] & \mathbb{Q}(\sqrt[3]{2}\omega^2) \arrow[dl, dash, "3"] & \mathbb{Q}(\omega) \arrow[dll, dash, "2"] \\
& \mathbb{Q} & &
\end{tikzcd}
\qquad
\begin{tikzcd}
& \{e\} \arrow[dl, dash, "3"'] \arrow[d, dash, "3"] \arrow[dr, dash, "3"] \arrow[drr, dash, "2"] & & \\
\langle(23)\rangle \arrow[dr, dash, "2"'] & \langle(13)\rangle \arrow[d, dash, "2"] & \langle(12)\rangle \arrow[dl, dash, "2"] & \langle(123)\rangle \arrow[dll, dash, "3"] \\
& S_3 & &
\end{tikzcd}$$

Thus all the $\mathbb{Q} \subset k$ such that $[k : \mathbb{Q}] = 3$ are

$$\{\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2})e^{\frac{2\pi i}{3}}, \mathbb{Q}(\sqrt[3]{2})e^{\frac{4\pi i}{3}}\}$$

(d) None of the above are normal because the subgroups

$$\{\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle\}$$

are all Sylow 2-subgroups of S_3, hence all conjugates to one another, i.e., not normal.

$\square$

Problem 12.4 (F2001-Q4). Let $K := \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

(a) Show that K is the splitting field of $X^4 - 6X^2 + 4$.

(b) Find the structure of the Galois group of $K/\mathbb{Q}$.

(c) List all the fields k, satisfying $\mathbb{Q} \subseteq k \subseteq K$.

Proof. (a) I belive there is typo in (a) where the polynomial should be $f(X) = X^4 - 16X^2 + 4$. This is the minimal polynomial of $\sqrt{3} + \sqrt{5}$. We see that $\mathbb{Q}(\sqrt{3} + \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$, hence it contains all the roots of f.

(b) We let $\alpha = \sqrt{3} + \sqrt{5}$, and $\beta = \sqrt{3} - \sqrt{5}$, then we see Galois group permutes

$$\{\alpha, -\alpha, \beta, -\beta\}$$

and we have $\alpha\beta \in \mathbb{Q}$. Thus just like the above, we have

$$\mathrm{Gal}(K/\mathbb{Q}) = \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$$

(c) We know the intermediate fields are determined by the subgroup of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$$\begin{tikzcd}
& \{e\} \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\langle(1,0)\rangle \arrow[dr, dash, "2"'] & \langle(1,1)\rangle \arrow[d, dash, "2"] & \langle(0,1)\rangle \arrow[dl, dash, "2"] \\
& \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &
\end{tikzcd}$$

and let $(1, 0)$ be the element such that

$$(1, 0) \cdot (\sqrt{3} + \sqrt{5}) = \sqrt{3} - \sqrt{5}$$

then we have the corresponding lattice of subfields

$$
\begin{tikzcd}
& \{e\} \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\langle(1,0)\rangle \arrow[dr, dash, "2"'] & \langle(1,1)\rangle \arrow[d, dash, "2"] & \langle(0,1)\rangle \arrow[dl, dash, "2"] \\
& \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} &
\end{tikzcd}
$$

$$
\begin{tikzcd}
& \mathbb{Q}(\sqrt{3},\sqrt{5}) \arrow[dl, dash, "2"] \arrow[d, dash, "2"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr, dash, "2"] & \mathbb{Q}(\sqrt{15}) \arrow[d, dash, "2"'] & \mathbb{Q}(\sqrt{5}) \arrow[dl, dash, "2"'] \\
& \mathbb{Q} &
\end{tikzcd}
$$

So all intermediate fields are

$$\left\{\mathbb{Q}(\sqrt{3}),\mathbb{Q}(\sqrt{15}),\mathbb{Q}(\sqrt{5})\right\}$$

□

Problem 12.5 (F2013-Q5)**.** Compute the Galois group of $f(x) = x^4 + 1$ over $\mathbb{Q}$.

Proof. The splitting field for f is $\mathbb{Q}(\xi_8)$ where $\xi_8 = e^{\frac{2\pi i}{8}}$, and the Galois group

$$\text{Gal}(\mathbb{Q}(\xi_8)/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times$$

thus

$$(\mathbb{Z}/8\mathbb{Z})^\times \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$$

□

Problem 12.6 (F2016-Q4)**.**

(1) Determine the Galois group of $x^4 - 4x^2 - 2$ over $\mathbb{Q}$.

(2) Let G be a group of order 8 such that G is the Galois group of a polynomial of degree 4 over $\mathbb{Q}$. Show that G is isomorphic to the Galois group in part (1).

Proof. (a) There are four roots of this polynomial

$$\{\alpha, -\alpha, \beta, -\beta\}$$

where

$$\alpha = \sqrt{2+\sqrt{6}}, \beta = \sqrt{2-\sqrt{6}}$$

Thus the Galois group embeds into S_4. Notice that

$$\alpha\beta = \sqrt{2}i$$

Thus we see the Galois extension has degree 8:

$$\begin{array}{c} \mathbb{Q}(\sqrt{2+\sqrt{6}}, \sqrt{2}i) \\ \Big| \, {\scriptstyle 2} \\ \mathbb{Q}(\sqrt{2+\sqrt{6}}) \\ \Big| \, {\scriptstyle 4} \\ \mathbb{Q} \end{array}$$

Notice that the Galois grop G is an order 8 subgruop of S_4, which implies that G is a Sylow 2 subgroup, and all Sylow 2 subgruops are isomorphic:

$$G \cong D_8$$

(b) The argument is given in (a).

□

Problem 12.7 (S2008-Q3). Let K be the splitting field of the polynomial $X^4 - 6X^2 - 1$ over $\mathbb{Q}$.

(a) Compute $\text{Gal}(K/\mathbb{Q})$.

(b) Determine all intermediate fields that are Galois over $\mathbb{Q}$.

Proof. (a) This computation is exactly same as above, as we have the four roots

$$\left\{\pm\sqrt{3+\sqrt{10}}, \pm\sqrt{3-\sqrt{10}}\right\}$$

and we see that $\alpha\beta = i$, thus the Galois group $\text{Gal}(K/\mathbb{Q})$ has order 8, and embeds into S_4, thus

$$\text{Gal}(K/\mathbb{Q}) \cong D_8$$

(b) not finished

□

Problem 12.8 (S2010-Q3). Compute Galois groups of the following polynomials.

(a) $x^3 + t^2x - t^3$ over k, where $k = \mathbb{C}(t)$ is the field of rational functions in one variable over complex numbers $\mathbb{C}$.

(b) $x^4 - 14x^2 + 9$ over $\mathbb{Q}$.

Proof. (a) The polynomial completely factors over $\mathbb{C}(t)$, so the Galois group is $\{e\}$.

(b) The roots are

$$\left\{\pm\sqrt{7 \pm 2\sqrt{10}}\right\}$$

and $\alpha\beta \in \mathbb{Q}$ again, hence the Galois group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

□

Problem 12.9 (S2013-Q6). Let K be the splitting field of $x^6 - 5$ over $\mathbb{Q}$.

(a) Prove that $x^6 - 5$ is irreducible over $\mathbb{Q}$.

(b) Compute the Galois group of K over $\mathbb{Q}$.

(c) Describe an intermediate field F such that F is not $\mathbb{Q}$ or K and $F/\mathbb{Q}$ is Galois.

Proof. (a) By Eisenstein.

(b) We know $K = \mathbb{Q}(\sqrt[6]{5}, \zeta_6)$, where ζ_6 is the 6th root of unity. The roots are

$$\left\{\sqrt[6]{5}, \sqrt[6]{5}\zeta_6, \ldots, \sqrt[6]{5}\zeta_6^5\right\}$$

Note that the minimal polynomial for ζ_6 is $x^2 - x + 1$, so the size of $\mathrm{Gal}(K/\mathbb{Q})$ is 12. We see that any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is determined by where it sends $\sqrt[6]{5}$ and ζ_6, so we only need to compute the possibilities of them. The Galois action is transitive implies that there $\sqrt[6]{5}$ can be sent to any $\sqrt[6]{5}\zeta_6^k$, where $k = 0, 1, 2, 3, 4, 5$, and since ζ_6 has minimal polynomial

$$x^2 - x + 1$$

Then there are two possibilities for $\zeta_6 \mapsto \zeta_6, \bar{\zeta}_6$, where $\bar{\zeta}_6 = \zeta_6^5$. Now we see that

$$\mathrm{Gal}(K/Q) = D_{12}$$

as it is generated by

$$\sigma : \sqrt[6]{5} \mapsto \zeta_6 \sqrt[6]{5}, \zeta_6 \mapsto \zeta_6, \quad \tau : \sqrt[6]{5} \mapsto \sqrt[6]{5}, \zeta_6 \mapsto \zeta_6^5$$

satisfying $\tau\sigma = \tau\sigma^{-1}$. (One can draw a hexagon)

(c) $F/\mathbb{Q}$ corresponds to a normal subgroup of D_{12}. Any subgroup of 6 is normal, i.e., the subgroup

$$\{e, \sigma, \ldots, \sigma^5\}$$

This subgroup fixes the field $\mathbb{Q}(\zeta_6)$. Hence it corresponds to

$$F = \mathbb{Q}(\zeta_6)$$

□

Problem 12.10 (S2016-Q3). Determine the Galois group of $x^6 - 10x^3 + 1$ over $\mathbb{Q}$.

Proof. This is the same process as above, the roots are

$$\left\{\zeta_3^i \sqrt[3]{5 \pm 2\sqrt{6}} : i = 0, 1, 2\right\}$$

The order of the Galois group G is 12, but now we need another trick.

Lemma 12.1. Transitive subgroup of S_6 of order 12 can only be D_{12} or A_4. However, A_4 has no index 2 subgroups, i.e., this Galois extension cannot have a subfield extension of degree 2 over $\mathbb{Q}$, this gives that G must be D_{12}:

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt[3]{2+\sqrt{6}}, \zeta_3) \arrow[dl, dash, "6"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\zeta_3) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt[3]{2+\sqrt{6}}) \arrow[dl, dash, "6"] \\
& \mathbb{Q} &
\end{tikzcd}$$

□

Problem 12.11 (F2010-Q3). Let $K = \mathbb{Q}(\sqrt[8]{2}, \sqrt{-1})$ and $F = \mathbb{Q}(\sqrt{-2})$. Show that K is Galois over F and determine the Galois group $\text{Gal}(K/F)$.

Proof. Since $\sqrt{2} = \zeta_8^4$, we see F is a subfield such that

$$\mathbb{Q} \subset F \subset K$$

Since K is Galois over $\mathbb{Q}$ (splitting field of $x^8 - 2$), we know K/F is also Galois. Now The Galois group $\text{Gal}(K/F)$ corresponds to the subgroup of $\text{Gal}(K/\mathbb{Q})$ which is D_{10} of index 5, i.e., a subgroup of order 2, hence

$$\text{Gal}(K/F) = \frac{\mathbb{Z}}{2\mathbb{Z}}$$

□

Problem 12.12 (F2015-Q2). The dihedral group D_{2n} is the group on two generators r and s, with respective orders $o(r) = n$ and $o(s) = 2$, subject to the relation $rsr = s$.

(a) Calculate the order of D_{2n}.

(b) Let K be the splitting field of the polynomial $x^8 - 2$. Determine whether the Galois group $\text{Gal}(K/\mathbb{Q})$ is dihedral (i.e., isomorphic to D_{2n} for some n).

Proof. (a) Because of the relation $srs = r^{-1}$, we can express all the terms in D_{2n} as

$$r^k s^m$$

where $0 \leq k \leq n-1, m = 0, 1$. Hence there are $2n$ elements.

(b) The Galois group is indeed diahedral, note that

$$K = \mathbb{Q}(\zeta_8, \sqrt[8]{2})$$

Thus $\text{Gal}(K/\mathbb{Q})$ has order 16 and the only transitive subgroup of S_8 of order 16 is D_{16}.

□

Problem 12.13 (S2019-Q1). Show that any transitive subgroup of A_5 is isomorphic to one of the following groups:

(a) the cyclic group $\mathbb{Z}/5\mathbb{Z}$,

(b) the dihedral group D_5,

(c) A_5.

Problem 12.14 (S2019-Q2). Let $f(x) = x^5 - 5x + 12$. Verify that $f(x)$ is irreducible in $\mathbb{Q}[x]$ and its discriminant is $d(f) = (2^6 5^3)^2$. If $r_1, \ldots, r_5$ are the roots of f, let

$$P(x) = \prod_{1 \le i < j \le 5} (x - (r_i + r_j)).$$

Show that $P(x)$ is a product of two monic irreducible polynomials in $\mathbb{Q}[x]$:

$$P(x) = (x^5 - 5x^3 - 10x^2 + 30x - 36)(x^5 + 5x^3 + 10x^2 + 10x + 4).$$

Use this information, Problem 1 and properties of $f_3 \in \mathbb{F}_3[x]$, the reduction of f modulo 3, to show that the the Galois group G_f of f is isomorphic to D_5.

Problem 12.15 (F2018-Q6). Determine the Galois group over $\mathbb{Q}$ of the polynomial

$$X^6 + 22X^5 - 9X^4 + 12X^3 - 37X^2 - 29X - 15.$$

Problem 12.16 (F2017-Q4). Compute the Galois group of $x^5 - 10x + 5$ over $\mathbb{Q}$.

Problem 12.17 (F2004-Q3). Let $f(x) = x^5 - 9x + 3$. Determine the Galois group of f over $\mathbb{Q}$.

Problem 12.18 (F2006-Q2). Let f be a polynomial in $\mathbb{Q}[x]$. Let E be a splitting field of f over $\mathbb{Q}$. For the following cases, determine whether E is solvable by radicals.

(1) $f(x) = x^4 - 4x + 2$.

(2) $f(x) = x^5 - 4x + 2$.

Problem 12.19 (S2011-Q3). Determine the Galois group [up to isomorphism] of the splitting field of each of the following polynomials over $\mathbb{Q}$:

(a) $f(x) = x^4 - 9x^3 + 9x + 4$,

(b) $g(x) = x^5 - 6x^2 + 2$.

Problem 12.20 (F2014-Q1).

(a) Let S_n be the symmetric group (permutation group) on n objects. Prove that if $\sigma \in S_n$ is an n-cycle and $\tau \in S_n$ is a transposition (i.e., a 2-cycle), then σ and τ generate S_n.

(b) Let $f_a(x)$ be the polynomial $x^5 - 5x^3 + a$. Determine an integer a with $-4 \le a \le 4$ for which f_a is irreducible over $\mathbb{Q}$, and the Galois group of [the splitting field of] f_a over $\mathbb{Q}$ is S_5. Then explain why the equation $f_a(x) = 0$ is not solvable in radicals.

(a) It suffices to assume that the n cycle is $(1 \ldots n)$ (up to rearranging the terms), and the transposition is (12). One can show that conjugation gives all the transpositions, hence generate S_n.

(b) Take $a = 1$, then $f_a(x)$ is irreducible: it doesn't have a root by the Rational Root Theorem and cannot be factored into lower degree polynomial by term matching. Moreover, we see that $f_a'(x)$ has 3 roots, by Rolle's theorem, there are at most 4 real roots, this implies that there exists a complex root r_1, and since this has odd degree, it must also exist a real root r_2. This shows that there exists an element in the Galois group that has order 5 and a transposition (sending conjugate complex roots to each other). Thus by (a), since the Galois group is a subgroup of S_5, we must have it equal to S_5.

Problem 12.21 (F2009-Q3). Determine the Galois group of $x^4 - 4x^2 + 7x - 3$ over $\mathbb{Q}$.

Problem 12.22 (S2012-Q3). In this problem, G denotes the group $S_5 \times C_2$, where S_5 is the symmetric group on five letters and C_2 is the cyclic group of order 2.

(a) Determine all normal subgroups of G.

(b) Give an example of a polynomial with rational coefficients whose Galois group is G, deducing that from basic principles.

Problem 12.23 (F2015-Q4). Let $H = S_3 \times S_5$.

(a) Determine all normal subgroups of H. Make sure you have them all! What would be different if H were replaced by $S_2 \times S_5$?

(b) Describe, in full detail, the construction of a polynomial with rational coefficients, whose Galois group is isomorphic to H.