Algebra Qualifying Exams

0.1 Spring 2018

1. Classify groups of order $2018 = 2 \cdot 1009$.

   Solution. Let G have order 2018. By Sylow's theorems, the number of Sylow-1009 subgroups is 1 mod 1009 and divides 2. There is then just one Sylow-1009 subgroup, which we denote by P. Again by Sylow's theorem, G acts transitively by conjugation on its Sylow subgroups of a given order, so P is normal in G.

   By the same reasoning, the number of Sylow-2 subgroups is either 1 or 1009. Any proper subgroup of G has order either 1009 or 2 by Lagrange's theorem. Furthermore, the Sylow-2 and Sylow-1009 subgroups intersect trivially as they are cyclic of relatively prime order. We conclude that there cannot be just one Sylow-2 subgroup, or else we would have only $1009+1$ elements in G.

   Now let Q be any Sylow-2 subgroup of G. Since P is normal in G, $P \cap Q = \{e\}$, and $|P| \cdot |Q| = |G|$, we have that G is a semidirect product of P and Q. Such a product is given by a homomorphism $\varphi : Q \to \operatorname{Aut}(P) \cong \mathbb{Z}/1008\mathbb{Z}$. Such a map must take the identity in Q to an element with order dividing 2. We can then have the trivial map $\varphi \equiv 0$ or $\varphi(1) = 504 \in \mathbb{Z}/1008\mathbb{Z}$. We conclude that there are exactly two groups of order 2018 up to isomorphism.

   $\mathbb{Z}/2018\mathbb{Z}$ and the dihedral group of order 2018, D_{1009}, are two non-isomorphic (D_{1009} is non-abelian by looking at its standard presentation) groups of order 2018, so this must be a complete list of such groups. □

2. Let P be a group of order $|P| = p^r$ for some prime p.

   (a) Prove that $Z(P) \neq 1$.

   Proof. We assume that $r > 0$. By the class equation (which itself follows from letting P act on itself by conjugation and applying the orbit-stabilizer theorem) we have that

   $$|P| = p^r = |Z(P)| + \sum_{i=1}^{k} [G : C_G(g_i)],$$

   where $g_1, \ldots, g_k$ are representatives from the distinct conjugacy classes of G not contained in the center and $C_G(g_i)$ is the centralizer of g_i. By Lagrange's theorem, each term $[G : C_G(g_i)]$ is also a prime power p^{e_i} for some $e_i > 0$ (if $e_i = 0$ then g_i would be in the center). Subtracting gives

   $$|Z(P)| = p^r - \sum_{i=1}^{k} [G : C_G(g_i)].$$

Reducing mod p shows that $|Z(P)|$ is a multiple of p. Since the center always contains the identity, we conclude that the center is nontrivial. □

(b) Prove that P is solvable.

Proof. We induct on k. If $r = 1$ then $P \cong \mathbb{Z}/p\mathbb{Z}$, which is abelian, and therefore solvable. Suppose then that the claim holds for all powers of p up to k and let $|P| = p^{k+1}$. If the center of P is all of P, then again P is abelian and solvable. Suppose then that P is not abelian. By part (a) we know that the center is nontrivial, so $P/Z(P)$ is a p-group with size strictly smaller than that of P. By the inductive hypothesis, $P/Z(P)$ and $Z(P)$ are solvable, so P is solvable. □

3. Let $\mathfrak{m} \subset R = \mathbb{Z}[x]$ be a maximal ideal. Prove that $R/\mathfrak{m}$ is a finite field. *Hint: first show that the image of $\mathbb{Z}$ is finite.*

Proof. Denote $k = R/\mathfrak{m}$ and let $\varphi : \mathbb{Z} \to k$ be the map that takes 1 to 1 (any ring admits such a map from $\mathbb{Z}$). We claim that this map is not injective. If it were, then it would have to extend to an injection $\Phi : \mathbb{Q} \to k$. Let $\pi : \mathbb{Z}[x] \to k$ be the projection map (which agrees with φ on $\mathbb{Z} \subseteq \mathbb{Z}[x]$). If we set $\Pi(x) = \pi(x)$ and $\Pi(q) = \Phi(q)$ for any $q \in \mathbb{Q}$ then we have a commutative diagram.

$$\begin{tikzcd}
\mathbb{Z}[x] \arrow[r, "\pi"] \arrow[d, hook] & k \\
\mathbb{Q}[x] \arrow[ur, "\Pi"] &
\end{tikzcd}$$

Π is surjective since π is, so by the first isomorphism theorem we have that $\mathbb{Q}[x]/\ker \Pi \cong k$. $\ker \Pi$ is then a maximal ideal of $\mathbb{Q}[x]$, so it has the form $(f(x))$ for some irreducible polynomial $f(x)$, which we can take to be primitive. Since $k \cong \mathbb{Q}[x]/(f(x))$, we have a surjection from $\mathbb{Z}[x]$ onto $\mathbb{Q}[x]/(f(x))$.

The kernel of this surjection is $\ker \Pi \cap \mathbb{Z}[x] = f(x)\mathbb{Q}[x] \cap \mathbb{Z}[x]$. By Gauss' lemma we have that $f(x)\mathbb{Q}[x] \cap \mathbb{Z}[x] = f(x)\mathbb{Z}[x]$, so we have an isomorphism $\mathbb{Z}[x]/(f(x)) \cong \mathbb{Q}[x]/(f(x))$. We claim that this can't happen since $\mathbb{Q}[x]/(f(x))$ is a field while $\mathbb{Z}[x]/(f(x))$, as we'll show, cannot be a field.

Choose $a \in \mathbb{Z}$ such that $f(a) \neq 0, \pm 1$ and let p be any prime dividing $f(a)$. If we let $\psi : \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}$ that sends x to a mod p, then $(f(x))$ is in the kernel of ψ, so we get another commutative diagram.

$$\begin{tikzcd}
\mathbb{Z}[x] \arrow[r, "\psi"] \arrow[d, two heads] & \mathbb{Z}/p\mathbb{Z} \\
\mathbb{Z}[x]/(f(x)) \arrow[ur, "\Psi"] &
\end{tikzcd}$$

$\mathbb{Z}/p\mathbb{Z}$ is a field, so if $\mathbb{Z}[x]/(f(x))$ is a field, then Ψ must be either injective or the zero map. But $\mathbb{Z}[x]/(f(x))$ is infinite in size, so Ψ must be identically zero. In particular, $\Psi(1) = 0$. By the commutativity of the diagram, we must have that for some $u(x), v(x) \in \mathbb{Z}[x]$,

$$1 = u(x)f(x) + v(x)p.$$

But substituting $x = a$ and reducing mod p gives a contradiction. We conclude that the image of $\mathbb{Z}$ in k is finite.

Since the image of $\mathbb{Z}$ in k is finite, we have that k has positive characteristic, say p. In particular, we have that $(p) \subset \mathfrak{m}$. Since $\mathbb{Z}[x]$ is Noetherian, we can write

$$\mathfrak{m} = (p, f_1(x), \ldots, f_k(x))$$

for some finite k, which gives

$$\mathbb{Z}[x]/\mathfrak{m} \cong (\mathbb{Z}/p\mathbb{Z})[x]/(f_1(x), \ldots, f_k(x)),$$

which is a finite field. □

4. Let R be a UFD and assume that any ideal in I is finitely generated. Suppose that for every nonzero a, b in R and any $d = \gcd(a, b)$ in R is expressible as $d = ra + sb$ for some $r, s \in R$. Prove that R is a PID.

5. Classify all finite abelian groups G such that $G \otimes_{\mathbb{Z}} (\mathbb{Z}/9\mathbb{Z}) \cong G$.

6. Let F be a field and let A and B be non-singular 3×3 matrices over F. Suppose that $B^{-1}AB = 2A$.

   (a) find the characteristic of F.

   (b) if n is a positive or negative integer not divisible by 3, prove that the matrix A^n has trace 0.

   (c) prove that the characteristic polynomial of A is $X^3 - a$ for some $a \in F$.

7. Let K be a field an let A be an $n \times n$ matrix over K. Suppose that $f \in K[x]$ is an irreducible polynomial such that $f(A) = 0$. Show that $\deg(f)|n$.

8. Let F be a field and $f(x) \in F[x]$ be irreducible. Let E be a splitting field of $f(x)$ over F. Suppose that a in E is such that a and $a+1$ are both roots of $f(x)$. Show that F doesn't have characteristic zero.

9. Let $\mathbb{F}_q$ be a finite field and let $\alpha \in \mathbb{F}_q^\times$. Let K be a splitting field over $\mathbb{F}_q$ of $X^{q+1} - \alpha$. Prove that $[K : \mathbb{F}_q] = 2$.

10. For the alternating group A_4

    (a) Classify the conjugacy classes of A_4.

    (b) Construct the character table of A_4.

0.2 Spring 2016

1. (a) Prove that every subgroup of a cyclic group is cyclic.

Proof. Let G be a cyclic group. First, suppose that G is of infinite order. Then sending the generator of G to $1 \in \mathbb{Z}$ gives an isomorphism $G \cong \mathbb{Z}$. We claim that every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$, which is clearly cyclic. Let H be a subgroup of G and let n be the smallest positive integer in H. Then $n\mathbb{Z} \subseteq H$. Suppose the containment is strict and let m be the smallest positive integer in $H \setminus n\mathbb{Z}$. We then have that $1 \leq \gcd(m, n) < n$ and by Bezout's identity we have that $\gcd(m, n) = um + vn$ for some $u, v \in \mathbb{Z}$ is in H. But this contradicts the minimality of n, so we conclude that $H = n\mathbb{Z}$.

Suppose now that $G = \langle g \rangle$ is finite of order n so that $G \cong \mathbb{Z}/n\mathbb{Z}$. By the fourth isomorphism theorem (or lattice/correspondence theorem) there is a one-to-one correspondence between subgroups of $\mathbb{Z}/n\mathbb{Z}$ and subgroups of $\mathbb{Z}$ containing $n\mathbb{Z}$. We have already shown that all subgroups of $\mathbb{Z}$ are cyclic, and since the homomorphic image of a cyclic group is cyclic ($\varphi(g^k) = \varphi(g)^k$), we have that all subgroups of $\mathbb{Z}/n\mathbb{Z}$ are cyclic. □

(b) Is the automorphism group of a cyclic group necessarily cyclic?

Solution. This need not be the case. Let $G \cong \mathbb{Z}/N\mathbb{Z}$. As G is cyclic, any automorphism of G is determined by where it sends a generator and it must map a generator to a generator. The generators of $\mathbb{Z}/N\mathbb{Z}$ exactly correspond to the elements of $(\mathbb{Z}/N\mathbb{Z})^\times$ and we have that $\text{Aut}(\mathbb{Z}/N\mathbb{Z}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. If N is a product of distinct primes $p, q > 2$ then the Chinese remainder theorem says that

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z},$$

which is not cyclic □

2. Let $G = \mathbb{Z}/25\mathbb{Z}$ be the cyclic group of order 25.

(a) Can G be given the structure of a $\mathbb{Z}[i]$-module?

Solution. Yes it can. Observe that in $\mathbb{Z}/25\mathbb{Z}$, $-1 = 24 = 6 \cdot 4 = 9^2 \cdot 2^2$, so $18^2 = -1$. Define the action of $a + bi \in \mathbb{Z}[i]$ on $m \in \mathbb{Z}/25\mathbb{Z}$ by

$$(a + bi) \cdot m = (a + 18b)m.$$

This action gives G the structure of a $\mathbb{Z}[i]$-module since

$$\begin{aligned}
[(a+bi)+(c+di)]\cdot m &= [(a+c)+(b+d)i]\cdot m \\
&= [(a+c)+18(b+d)]m \\
&= (a+bi)\cdot m + (c+di)\cdot m. \\
(a+bi)\cdot(m+n) &= (a+18b)(m+n) \\
&= (a+bi)\cdot m + (a+bi)\cdot n. \\
[(a+bi)(c+di)]\cdot m &= [(ac-bd)+(ad+bc)i]m \\
&= [(ac-bd)+18(ad+bc)]m \\
&= (a+bi)\cdot[(c+di)\cdot m].
\end{aligned}$$

□

(b) Can G be given the structure of a $\mathbb{Z}/5\mathbb{Z}$ module?

Solution. No it cannot. If it could then we would have

$$\begin{aligned}
0 &= 0\cdot 1 \\
&= 5\cdot 1 \\
&= (1+1+1+1+1)\cdot 1 \\
&= 1\cdot 1 + 1\cdot 1 + 1\cdot 1 + 1\cdot 1 + 1\cdot 1 \\
&= 5 \\
&\neq 0.
\end{aligned}$$

□

3. Prove that there is no simple group of order 520.

Proof. Write $520 = 2^3 \cdot 5 \cdot 13$. By Sylow's theorems, the number of Sylow-5 subgroups, n_5 is 1 mod 5 and divides $2^3 \cdot 13 = 104$. The only positive integers satisfying these constraints are 1 and 26. The same reasoning shows that n_{13} must be 1 or 40. If either of n_5 or n_{13} is 1, then since Sylow-p subgroups are conjugate to one another, then that subgroup would be normal. Suppose then that $n_5 = 26$ and $n_{13} = 40$. Then there are $26 \cdot 4 = 104$ elements of order 5 and $40 \cdot 12 = 480$ elements of order 13. But $104 + 480 = 584 > 520$, so this cannot be the case. We conclude that there must be a unique Sylow-5 or Sylow-13 subgroup which is normal. □

4. Let G be a finite group acting transitively on a set X with $|X| > 1$.

   (a) State the orbit-stabilizer theorem.

   Solution. If a group G acts on a set X then for any $x \in X$, the size of the orbit of x under G is the index of the stabilizer of x under G, $|\mathcal{O}(x)| = [G : \mathrm{Stab}(x)]$. □

   (b) Show that there is some element of G fixing no element of X.

   Proof. Since the action of G on X is transitive there is a single orbit. Burnside's lemma (which immediately follows from the orbit-stabilizer theorem) then states that

$$1 = \frac{1}{|G|} \sum_{g \in G} |\{x \in X : g \cdot x = x\}|.$$

   If $g \in G$ has fixed points then it contributes at least $1/|G|$ to the above sum. If *every* element has a fixed point then we must have that every term in the sum is $1/|G|$. But the identity element fixes every element in X and $|X| > 1$, so we must have that one term in this sum is zero, i.e. at least one element of G is fixed point free. □

5. Let K be a field and let $\overline{K}$ be an algebraic closure of K. Assume $\alpha, \beta \in \overline{K}$ have degree 2 and 3 over K, respectively.

   (a) Can $\alpha\beta$ have degree 5 over K?

   Solution. No it cannot. We have that $K(\alpha\beta)$ is contained in the composite extension $K(\alpha)K(\beta)$. Furthermore, since the degrees of $K(\alpha)$ and $K(\beta)$ over K are relatively prime, we have that the composite extension has degree 6 over K. Since $K(\alpha\beta)$ is a subfield of the composite extension, its degree over K must divide 6. Since 5 doesn't divide 6 we have that $K(\alpha\beta)$ cannot have degree 5 over K. □

   (b) Can $\alpha\beta$ have degree 6 over K?

   Solution. Yes it can. Consider $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$. $x^2 - 2$ and $x^3 - 2$ are irreducible over $\mathbb{Q}$ by Eisenstein so these extensions are of degree 2 and 3, respectively. We claim that the product $2^{1/2} \cdot 2^{1/3} = 2^{5/6}$ has degree 6 over $\mathbb{Q}$.

   We start by showing that $\mathbb{Q}(2^{5/6}) = \mathbb{Q}(2^{1/6})$. Clearly $\mathbb{Q}(2^{5/6}) \subseteq \mathbb{Q}(2^{1/6})$. On the other hand, $\frac{1}{2^4}(2^{5/6})^5 = 2^{1/6}$, so $\mathbb{Q}(2^{1/6}) \subseteq \mathbb{Q}(2^{5/6})$. Finally, $2^{1/6}$ is a root of the polynomial $x^6 - 2$, which is irreducible over $\mathbb{Q}$ by Eisenstein, so we have that $2^{1/6}$, and therefore $2^{5/6}$, has degree 6 over $\mathbb{Q}$. □

6. Let $L/\mathbb{Q}$ denote a Galois extension with Galois group isomorphic to A_4.

   (a) Does there exist a quadratic extension $K/\mathbb{Q}$ contained in L?

Solution. By the fundamental theorem of Galois theory, a quadratic extension $K/\mathbb{Q}$ corresponds to a subgroup of $\mathrm{Gal}(L/\mathbb{Q}) \cong A_4$ of index 2 (order 6). We claim that there is no such subgroup, and therefore no such quadratic sub-extension.

Any group of order 6 is isomorphic to either $\mathbb{Z}/6\mathbb{Z}$ or S_3. A_4 consists of double 2-cycles, e.g. $(1\ 2)(3\ 4)$, and 3-cycles, e.g. $(1\ 2\ 3)$, none of which have order 6, so that leaves S_3. S_3 has three elements of order 2, and since the three double 2-cycles in A_4 are exactly its elements of order 2, they must all lie in any subgroup isomorphic to S_3. However, the elements of order 2 don't commute with one another in S_3 while they do in A_4, so we cannot have a subgroup of A_4 isomorphic to S_3. □

(b) Does there exist a degree 4 polynomial in $\mathbb{Q}[x]$ with splitting field equal to L?

Solution. □

7. Let $A : V \to V$ be a linear transformation of a vector space V over the field $\mathbb{Q}$ which satisfies the relation $(A^3 + 3I)(A^3 - 2I) = 0$. Show that the dimension $\dim_{\mathbb{Q}}(V)$ is divisible by 3.

Proof. Since A satisfies the polynomial $(x^3+3)(x^3-2)$, the minimal polynomial of A over $\mathbb{Q}$ must divide $(x^3+3)(x^3-2)$. Since x^3+3 and x^3-2 are both irreducible over $\mathbb{Q}$ by Eisenstein, the minimal polynomial must be either x^3+3, x^3-2 or $(x^3+3)(x^3-2)$. Furthermore, the minimal polynomial divides the characteristic polynomial whose degree is the dimension of V over $\mathbb{Q}$. Since the minimal polynomial and characteristic polynomial have the same roots in an algebraic closure, we must have that the characteristic polynomial is of the form $(x^3+3)^a(x^3-2)^b$ for some nonnegative integers a, b at least one of which is positive. Since the degree of such a polynomial is divisible by 3, we must have that the dimension of V over $\mathbb{Q}$ is divisible by 3. □

8. True/False.

(a) If K_1, K_2 are fields and $\varphi : K_1 \to K_2$ is a ring homomorphism such that $\varphi(1) = 1$, then φ is injective.

Solution. True. The kernel of φ is an ideal in K_1. Since K_1 is a field its only ideals are (0) and all of K_1. Since $\varphi(1) = 1$, we have that the kernel of φ is not all of K_1, so it must be trivial, forcing φ to be injective. □

(b) The unit group of $\mathbb{C}$ is isomorphic to the additive group of $\mathbb{C}$.

Solution. Assuming "the unit group of $\mathbb{C}$" means the nonzero complex numbers, $\mathbb{C}^\times$, then this is false. $\mathbb{C}^\times$ contains an element of order 2, -1, whereas the additive group $(\mathbb{C}, +)$ contains no elements of order 2. □

(c) Let n be a positive integer. Then $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.

Solution. True. For any simple tensor $a \otimes \frac{p}{q}$ in $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$ we have

$$\begin{aligned} a \otimes \frac{p}{q} &= a \otimes \frac{np}{nq} \\ &= na \otimes \frac{p}{nq} \\ &= 0 \otimes \frac{p}{nq} \\ &= 0. \end{aligned}$$

□

9. For each of the following either give an example or show that none exists.

(a) An element $\alpha \in \mathbb{Q}(\sqrt{2}, i)$ such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i)$.

Solution. As this is a finite extension of $\mathbb{Q}$ and since any such extension is separable as $\mathbb{Q}$ is perfect, the primitive element theorem guarantees the existence of such an α. We claim that $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$. The inclusion $\mathbb{Q}(\sqrt{2} + i) \subseteq \mathbb{Q}(\sqrt{2}, i)$ is obvious. Note that $(\sqrt{2} + i)^3 = -\sqrt{2} + 5i$. This gives

$$(\sqrt{2} + i)^3 + (\sqrt{2} + i) = 6i,$$

so $i \in \mathbb{Q}(\sqrt{2} + i)$. Subtracting i from $\sqrt{2} + i$ shows that $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + i)$ as well and we have the reverse inclusion. □

(b) A tower of field extensions $L \supseteq K' \supseteq K$ such that L/K' and K'/K are Galois extensions but L/K is not Galois.

Solution. Consider the extensions $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$. Both of these extensions are Galois since they are quadratic. However, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not Galois because it doesn't contain the non-real roots of $x^4 - 2$. □

10. Let $L_1, \ldots, L_r$ be all pairwise non-isomorphic complex irreducible representations of a group G of order 12. What are the possible values for their dimensions $n_i = \dim_{\mathbb{C}} L_i$? For each of the possible answers of the form $(n_1, \ldots, n_r)$ give an example of G which has such irreducible representations.

Solution. We have that $n_1^2 + \cdots + n_r^2 = 12$ and that r is the number of conjugacy classes in G. Since the one-dimensional trivial representation is always a representation of G, we know that at least one of the n_i is 1. We also know that the number of conjugacy classes divides the order of G by Lagrange's theorem. These constraints give us three possible configurations of the n_i:

$$(1,1,1,1,1,1,1,1,1,1,1,1) \quad (1,1,1,1,2,2) \quad (1,1,1,3).$$

Here are some examples from each class.

$(1,\ldots,1)$: The irreducible representations of an abelian group are all one-dimensional, so a group like $\mathbb{Z}/12\mathbb{Z}$ would fall into this category.

$(1,1,1,1,2,2)$: We can safely place the dihedral group D_{12} in this category because it has six conjugacy classes and this is the only configuration of the n_i consistent with this.

$(1,1,1,3)$: The alternating group A_4 is in this category because it has four conjugacy classes.

□

0.3 Fall 2015

1. (a) Define **prime ideal**.

Solution. An ideal $P \neq R$ of the commutative ring R is prime if $ab \in R$ implies that $a \in R$ or $b \in R$. Equivalently, P is prime if and only if R/P is an integral domain. □

(b) Define **maximal ideal**.

Solution. An ideal $I \neq R$ of the ring R is maximal if I is not properly contained in another ideal (that isn't all of R). If R is commutative, then I is maximal if and only if R/I is a field. □

(c) Give an example of a ring R and ideal P_1, P_2, and P_3 of R such that for the properties "prime ideal" and "maximal ideal" of R,

i. P_1 satisfies both properties,

ii. P_2 satisfies neither property

iii. P_3 satisfies one property but not the other.

Solution. Let $R = \mathbb{Q}[x,y]$. The ideal $P_1 = (x,y)$ is maximal since $R/P_1 = \mathbb{Q}$, which is a field. Since all fields are integral domains, we have that P_1 is prime as well.

The ideal $P_2 = (x^2)$ is not prime since $x \cdot x$ is in P_2 but x is not. Since maximal ideals are always prime, this shows that P_2 isn't maximal either.

The ideal $P_3 = (x)$ is prime but not maximal since $R/P_3 = \mathbb{Q}[y]$, which is an integral domain but not a field. □

2. Show that if a group G has only finitely many subgroups then G is a finite group.

Proof. Suppose G is an infinite group. If G has an element g of infinite order then $\langle g\rangle \cong \mathbb{Z}$, which has infinitely many subgroups. Suppose then that every element of G has finite order. Since $G = \cup_{g\in G}\langle g\rangle$ and every $\langle g\rangle$ is a finite set, the only way to cover the infinite set G by finite sets $\langle g\rangle$ is to have infinitely many distinct $\langle g\rangle$. Thus, an infinite group must have infinitely many subgroups, so a group with finitely many subgroups must be finite. $\square$

3. Let A be an $n \times n$ matrix with entires in $\mathbb{R}$ such that $A^2 = -I$.

   (a) Prove that n is even.

   Proof. Since A satisfies the polynomial $x^2 + 1$, its minimal polynomial over $\mathbb{R}$ must divide $x^2 + 1$. This polynomial is irreducible over $\mathbb{R}$ and since the minimal polynomial divides the characteristic polynomial and both polynomials have the same roots in $\mathbb{C}$, the characteristic polynomial must be $(x^2 + 1)^d$ for some $d \geq 1$. The degree of the characteristic polynomial, $2d$, is n, so n is even. $\square$

   (b) Prove that A is diagonalizable over $\mathbb{C}$ and describe the corresponding diagonal matrices.

   Proof. The minimal polynomial of A, x^2+1 splits completely into distinct linear factors over $\mathbb{C}$, $(x+i)(x-i)$, so A is diagonalizable over $\mathbb{C}$. The Jordan blocks of A are all of size 1, so A is similar to a diagonal matrix with an equal number of i's and $-i$'s along the diagonal. $\square$

4. Let G be a group of order 70. Prove that G has a normal subgroup of order 35.

Proof. Any subgroup of G with order 35 will be normal as it will have index 2. It then suffices to simply show that G has a subgroup of order 35.

$70 = 2 \cdot 5 \cdot 7$. By Sylow's theorem, the number of Sylow-7 subgroups, n_7 is 1 mod 7 and divides $2 \cdot 5 = 10$. The only possibility is $n_7 = 1$. Similarly we have that $n_5 = 1$ as well. Since the Sylow-p subgroups are conjugate to one another, the fact that we have unique Sylow-5 and Sylow-7 subgroups shows that these subgroups, H and K, are normal in G. Consequently, the product subgroup HK is a subgroup of G with order

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

Since H and K are cyclic with relatively prime orders they must intersect trivially, so $|HK| = 35$. $\square$

5. Construct a Galois extension F of $\mathbb{Q}$ satisfying $\text{Gal}(F/\mathbb{Q}) \cong D_8$.

Solution. Consider the splitting field of $p(x) = x^4 - 2$ over $\mathbb{Q}$. p has roots $i^k 2^{1/4}$ for $k = 0, 1, 2, 3$, so $F = \mathbb{Q}(2^{1/4}, i)$. $\mathbb{Q}(2^{1/4})$ is a real degree 4 subextension. $[\mathbb{Q}(2^{1/4}, i) : \mathbb{Q}(2^{1/4})] = 2$, so we have that $[\mathbb{Q}(2^{1/4}, i) : \mathbb{Q}] = 8$. Since $\mathrm{Gal}(F/\mathbb{Q})$ is the Galois group of a degree-4 polynomial, it must be a subgroup of S_4. Any order 8 subgroup of S_4 is one of its (all isomorphic) Sylow-2 subgroups. The dihedral group D_8 is an order 8 subgroup of S_4, so we must have that $\mathrm{Gal}(F/\mathbb{Q}) \cong D_8$. □

6. Let F be a field. Prove that every ideal of $F[x]$ is principal.

Proof. Let I be a nonzero proper ideal of $F[x]$ and let a be an element of I of minimal degree. If $\deg a = 0$ then a is a unit, in which case $I = F[x]$. We claim that a divides every element of I, so since (a) is clearly contained in I, we'll have that $I = (a)$. Let b be any element of I. Since F is a field we can perform polynomial division with remainder to obtain unique q and r with $b = aq + r$, where r is either zero or has degree strictly less than that of a. r cannot have degree strictly less than that of a because a was chosen to have minimal degree, so we must have that $r = 0$ and a divides every element of I. □

7. Give an example of a module M over a ring R such that M is not finitely generated as an R-module.

Proof. Any infinitely generated abelian group will do the trick, e.g. $\bigoplus_{\mathbb{N}} \mathbb{Z}$. Abelian groups are $\mathbb{Z}$-modules, so an infinitely generated abelian group is not a finitely generated $\mathbb{Z}$-module.

Suppose $\bigoplus_{\mathbb{N}} \mathbb{Z}$ is finitely generated. Elements of this module are of the form $(a_i)_{i=1}^{\infty}$ where all but finitely many of the a_i are zero. If we could find a finite generating set of this module, there would be some maximal N with a_N nonzero an $a_j = 0$ for all $j > N$ and all generators (a_i). But $\bigoplus_{\mathbb{N}} \mathbb{Z}$ clearly contains elements where $a_j \neq 0$ for $j > N$, so this module cannot be finitely generated. □

8. Suppose H is a normal subgroup of a finite group G.

   (a) Prove or disprove: If H has order 2, then H is a subgroup of the center of G.

   Solution. This is true. Write $H = \{e, h\}$ where $h \neq e$. Since H is normal, ghg^{-1} is in H for all $g \in G$. If $ghg^{-1} = e$ then cancellation forces $h = e$, which isn't true, so we must have $ghg^{-1} = h$, which implies that $gh = hg$ for all g, which puts H in the center of G. □

   (b) Prove or disprove: If H has order 3, then H is a subgroup of the center of G.

   Solution. This is not true. Consider the symmetric group $S_3 = \langle r, s : r^3 = s^2 = e,\ rs = sr^2 \rangle$. The subgroup generated by r has order 3 and is normal since it has index 2 in S_3. However, it is not in the center of S_3 as $rs = sr^2 \neq sr$. □

9. (a) What does it mean for a representation to be irreducible?

Solution. A representation of G is irreducible if it contains no proper subrepresentations, i.e. V is irreducible if there is no proper subspace W of V invariant under G. □

(b) Suppose p is a prime. Let $G = \mathbb{Z}/p\mathbb{Z}$ and let $\rho : G \to \mathrm{GL}_2(\mathbb{F}_p)$ be a representation. Show that ρ is reducible.

Solution. Let V be a subspace of $\mathbb{F}_p^2$ fixed by G. If we let G act on $V \setminus \{0\}$ by ρ, the orbit stabilizer theorem tells us that the size of the orbit $|\mathcal{O}_x|$ divides the order of $\mathbb{Z}/p\mathbb{Z}$, p, for each $x \in V \setminus \{0\}$. The orbits partition $V \setminus 0$, so if we add up the sizes of each orbit we will get the size of $V \setminus \{0\}$, which is $p^n - 1$ for $n = 0$, 1, or 2. Since the size of each orbit is a divisor of p, there must be at least one orbit of size 1, i.e. a vector fixed by the action of G. But then the span of this vector is a subspace of V invariant under G: a proper subrepresentation. □

10. (a) Compute the order of $\mathrm{GL}_4(\mathbb{F}_{3^2})$.

Solution. The first row in an element of $\mathrm{GL}_4(\mathbb{F}_9)$ can be any nonzero vector, of which there are $9^4 - 1$. The second row can be any vector not in the span of the first one, of which there are $9^4 - 9$. Continuing in this fashion, the i-th row can be any vector not in the span of the first $i - 1$ rows, which gives

$$|\mathrm{GL}_4(\mathbb{F}_9)| = (9^4 - 1)(9^4 - 9)(9^4 - 9^2)(9^4 - 9^3).$$

□

(b) Compute the order of $\mathrm{SL}_4(\mathbb{F}_{3^2})$.

Solution. $\mathrm{SL}_4(\mathbb{F}_9)$ is the kernel of the determinant map $\det : \mathrm{GL}_4(\mathbb{F}_9) \to \mathbb{F}_9^\times$. We can construct invertible matrices with any desired nonzero determinant by using diagonal matrices if we like, so this map is surjective. By the first isomorphism theorem we then have

$$\frac{|\mathrm{GL}_4(\mathbb{F}_9)|}{|\mathrm{SL}_4(\mathbb{F}_9)|} = |\mathbb{F}_9^\times|.$$

By part (a) we have

$$|\mathrm{SL}_4(\mathbb{F}_9)| = \frac{1}{8}(9^4 - 1)(9^4 - 9)(9^4 - 9^2)(9^4 - 9^3).$$

□

(c) Show that $\mathbb{Z}[\sqrt{10}]$ is not a UFD.

Solution. Observe that $10 = 2 \cdot 5 = \sqrt{10} \cdot \sqrt{10}$. If we can show that 2, 5, and $\sqrt{10}$ are irreducible in $\mathbb{Z}[\sqrt{10}]$ then we will have exhibited two decompositions of 10 into non-associate irreducible factors.

Define the norm $N(a+b\sqrt{10}) = a^2 - 10b^2$. It's easy to see that $N(\alpha\beta) = N(\alpha)N(\beta)$ and that $N(\alpha) = \pm 1$ if and only if α is a unit. Now $N(2) = 4 = 2^2$. If we can show that there are no elements with norm ± 2 then we will have shown that 2 is irreducible.

Suppose $N(\alpha) = a^2 - 10b^2 = \pm 2$. Reducing mod 4 we have $a^2 + 2b^2 \equiv 2 \pmod 4$. x^2 can only be zero or 1 mod 4, the former if x is even and the latter if x is odd. We conclude that a must be even and b odd. Substitute $a = 2m$ and $b = 2n+1$ to obtain

$$4m^2 - 10(4n^2 + 4n + 1) = \pm 2$$

$$\iff 4(m^2 - 10n^2 - 10n) - 10 = \pm 2$$

$$\iff m^2 - 10n^2 - 10n = 2 \text{ or } 3.$$

Reducing mod 10 we have $m^2 \equiv 2$ or 3 mod 10, which has no solutions. We conclude that no element of $\mathbb{Z}[\sqrt{10}]$ has norm ± 2, so 2 is irreducible.

Now we'll show that 5 is irreducible. $N(5) = 25 = 5^2$, so let's show that there are no elements with norm ± 5. Reducing $a^2 - 10b^2 = \pm 5$ mod 5 we have that a must be a multiple of 5. Substituting $a = 5m$ and dividing by 5 gives $5m^2 - 2b^2 = \pm 1$. Again, reducing mod 5 we obtain

$$3b^2 \equiv \pm 1 \pmod 5$$

$$\iff b^2 \equiv \pm 3 \pmod 5,$$

which has no solutions. We conclude that no element has norm ± 5, so 5 is irreducible.

Since $N(\sqrt{10}) = -10 = -2 \cdot 5$, we have also shown that $\sqrt{10}$ is irreducible. Thus, the decompositions $10 = 2 \cdot 5 = \sqrt{10} \cdot \sqrt{10}$ are non-associate irreducible decompositions, so $\mathbb{Z}[\sqrt{10}]$ is not a UFD. □

0.4 Spring 2015

1. Prove that every finite group of order > 2 has a nontrivial automorphism.

   Proof. Let G be a finite group with $|G| > 2$. If G is not abelian then conjugation by a non-identity element defines a non-trivial automorphism on G. If G is abelian and there is at least one element with order not equal to 2, then $x \mapsto x^{-1}$ defines a non-trivial automorphism of G. This leaves the case where G is abelian and every element of G has order 2. By the structure theorem for finitely generated abelian groups we have that

$$G \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2\mathbb{Z},$$

where there are finitely many factors. In this case, any non-identity permutation of the generators gives a non-trivial automorphism of G. □

2. (a) Define UFD.

   Solution. A UFD is an integral domain in which every element can be factored into irreducible elements that are unique up to multiplication by a unit. □

   (b) Define PID.

   Solution. A PID is an integral domain in which every ideal is generated by a single element. □

   (c) For the properties "UFD" and "PID", give an example of a commutative integral domain that

   i. satisfies both properties

   Solution. Every PID is a UFD, so any PID like $\mathbb{Z}$ will satisfy both properties. □

   ii. satisfies one property but not the other

   Solution. $\mathbb{Q}[x, y]$ is a UFD but not a PID. □

   iii. satisfies neither property

   Solution. $\mathbb{Z}[\sqrt{-5}]$ is the go-to example of an integral domain that isn't a UFD since $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ even though 2, 3, and $1 \pm \sqrt{-5}$ are all irreducible. □

3. (a) Prove that $\mathbb{Q}(\sqrt[4]{T})$ is not Galois over $\mathbb{Q}(T)$ where T is an indeterminate.

   Proof. $T^{1/4}$ is a root of the polynomial $x^4 - T$ defined over $\mathbb{Q}(T)$. An automorphism of $\mathbb{Q}(T^{1/4})$ over $\mathbb{Q}(T)$ is determined by where it sends $T^{1/4}$ and only two of the four possibilities, the other roots of $x^4 - T$, $\{\pm T^{1/4}, \pm iT^{1/4}\}$, lie in the field. Since there are only two automorphisms and the degree of the extension is four, the extension is not Galois. □

   (b) Find the Galois closure of $\mathbb{Q}(\sqrt[4]{T})$ over $\mathbb{Q}(T)$ and determine the Galois group both as an abstract group and as a set of explicit automorphisms.

   Proof. Since $T^{1/4}$ has minimal polynomial $x^4 - T$, the Galois closure is the splitting field of this polynomial. We claim that this field is $\mathbb{Q}(T^{1/4}, i)$. $\mathbb{Q}(T^{1/4}, i)$ clearly contains the splitting field and since

$$(iT^{1/4})/T^{1/4} = i,$$

   this field is contained in the splitting field, so they are one and the same.

Now to compute the Galois group. Since $\mathbb{Q}(T^{1/4})$ is a real field, $\mathbb{Q}(T^{1/4}, i)$ is quadratic over it, so $[\mathbb{Q}(T^{1/4}, i) : \mathbb{Q}(T)] = 8$. Since the Galois group permutes the four roots of the polynomial $x^4 - T$, it is a subgroup of S_4 with order 8. Such a subgroup is one of the Sylow-2 subgroups of S_4, all of which are isomorphic to one another. Since $D_8 \leq S_4$ has order 8, we must have that the Galois group, Γ, is isomorphic to D_8.

Let ρ be the map that multiplies each root $\{\pm T^{1/4}, \pm i T^{1/4}\}$ by i and let σ be the map that sends each root to its complex conjugate. These maps clearly fix the base field $\mathbb{Q}(T)$ and we have $\rho^4 = \sigma^2 = \text{id}$. A quick computation also shows that $\rho\sigma = \sigma\rho^3$: the relations defining D_8. □

4. Let R be a commutative ring with multiplicative identity. An element $r \in R$ is called nilpotent if there exists a positive integer n such that $r^n = 0$.

   (a) Prove that every nilpotent element lies in every prime ideal.

   Proof. Let P be a prime ideal, r a nilpotent element of R, and n the minimal positive integer such that $r^n = 0$. Since P contains zero and $r \cdot r^{n-1} = 0 \in P$, we have that P contains r or r^{n-1} since P is prime. If P contains r then we're done. If P contains r^{n-1}, then the primality of P says that P contains one of r or r^{n-2}. By induction, P must contain r. □

   (b) Assume that every element of R is either nilpotent or a unit. Prove that R has a unique prime ideal.

   Proof. Let P be a prime ideal. P can't contain a unit or else it would contain all of R, and by part (a) it must contain every nilpotent element. But R has only units and nilpotent elements, so P must consist exactly of the nilpotent elements. There can be only one such P. □

5. For every positive integer n, denote by C_n a cyclic group of order n and by D_n a dihedral group of order $2n$, so that

$$D_n = \{1, a, a^2, \ldots, a^{n-1}, b, ba, \ldots, ba^{n-1}\},$$

   where a has order n, b has order 2 and $ab = ba^{-1}$.

   (a) In the notation explained above, prove that every subgroup of $\langle a \rangle$ is normal in D_n.

   Proof. $\langle a \rangle$ is normal in D_n since it has index 2. Since this subgroup is cyclic of order n, it has a unique subgroup for each divisor d of n and this subgroup has order d. If a subgroup is the only subgroup with a given order then it is characteristic because an automorphism must send a subgroup of some order to another subgroup with the same order. We conclude that each subgroup of $\langle a \rangle$ is characteristic in $\langle a \rangle$. A characteristic subgroup of a normal subgroup is normal, so each of these subgroups is normal in D_n. □

(b) If $n = 2m$ with m odd, prove that $D_n = D_{2m} \cong C_2 \times D_m$.

Proof. First let's show that D_{2m} contains subgroups isomorphic to C_2 and D_m. Let $H = \langle b, a^2 \rangle$ and let $K = \langle r^m \rangle$. It's clear that $H \cong D_m$ and $K \cong C_2$. Since m is odd, $H \cap K$ contains only the identity element. H is normal in D_n since it has index two and K is normal by part (a).

Since H and K are normal and $H \cap K$ is trivial, we have that $HK \cong H \times K$. Furthermore, since

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = |H| \cdot |K| = D_n,$$

we have that $D_n \cong H \times K = D_m \times C_2$. □

(c) Is $D_{12} \cong C_3 \times D_4$?

Proof. It is not. Since C_3 has no elements of order 2, the elements of $C_3 \times D_4$ of order 2 are of the form (e, k), where $k \in D_4$ has order 2. In particular, this product has just as many elements of order 2 as D_4 does. D_4 (when viewed as the symmetries of the square) has five elements of order 2: the rotation through an angle of π, the two flips through opposite faces, and the two flips through opposite vertices. However, D_{12}, when viewed as the symmetries of a dodecagon, has at least seven elements of order 2: the π-rotation and six flips through opposite faces. □

6. Suppose that p and q are prime numbers with $p < q$. Prove that no group of order p^2q is simple.

Proof. Let G be a group of order p^2q. By Sylow's theorem, the number of Sylow-q subgroups is 1 mod q and divides p^2. Since $p < q$, we have that n_q is 1 or p^2. If $n_q = 1$ then the unique Sylow-q subgroup is normal and we're done. Suppose then that $n_q = p^2$. Each Sylow-q subgroup is isomorphic to $\mathbb{Z}/q\mathbb{Z}$, so these subgroups intersect trivially, giving us $p^2(q-1) = p^2q - p^2$ non-identity elements. This leaves room for only p^2 other elements, and since we have at least one Sylow-p subgroup, which must have order p^2, we conclude that there is only one such subgroup, forcing it to be normal. □

7. Determine the maximal ideals of the following rings.

(a) $\mathbb{Q}[x]/(x^2 - 5x + 6)$,

Solution. By the Chinese remainder theorem we have

$$\mathbb{Q}[x]/(x^2 - 5x + 6) \cong \mathbb{Q}[x]/(x-2) \oplus \mathbb{Q}[x]/(x-3) \cong \mathbb{Q} \oplus \mathbb{Q}.$$

The maximal ideals in a sum of rings $R \oplus S$ are of the form $M \oplus S$ or $R \oplus N$, where M is maximal in R and N is maximal in S. Since $\mathbb{Q}$ is a field, its only maximal ideal is (0), so the maximal ideals of this ring are $\mathbb{Q} \oplus (0)$ and $(0) \oplus \mathbb{Q}$. □

(b) $\mathbb{Q}[x]/(x^2+4x+6)$.

Solution. The discriminant of this quadratic is $4^2-4(1)(6) < 0$, so the quadratic is irreducible. Consequently, this quotient is a field, so its only maximal ideal is (0). □

8. Find two matrices having the same characteristic polynomials and minimal polynomials but different Jordan canonical forms.

Solution. Let the matrix A have invariant factors $\{(x-2)^2,\ (x-2)^2\}$ and let the matrix B have the invariant factors $\{(x-2),\ (x-2),\ (x-2)^2\}$. A and B both have the same minimal polynomial, $(x-2)^2$, and the same characteristic polynomial, $(x-2)^4$, but their Jordan forms are

$$A \sim \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}, \quad B \sim \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}.$$

□

9. (a) What does it mean for a field to be perfect?

Solution. A field is perfect if every finite extension of it is separable. □

(b) Given an example of a perfect field.

Solution. $\mathbb{Q}$ is perfect. To see this, note that any finite extension of $\mathbb{Q}$ is of the form $\mathbb{Q}[x]/(p(x))$, where $p(x)$ is an irreducible polynomial. Irreducible polynomials over $\mathbb{Q}$ (or any field of characteristic zero) have no repeated roots, so they are separable. □

(c) Give an example of a field that is not perfect.

Solution. $\mathbb{F}_2(t)$ is not perfect. Consider the polynomial x^2-t. This polynomial is irreducible, but its derivative is identically zero (it factors as $(x-\sqrt{t})^2$). □

10. (a) Classify the conjugacy classes of the symmetric group S_3.

Solution. Two elements of a symmetric group are conjugate if and only if they have the same cycle type, so the conjugacy classes of S_3 are the identity, the two-cycles, and the three-cycles. □

(b) Construct the character table of S_3.

Solution. S_3 has three conjugacy classes, so it has three irreducible complex representations. Any group has the trivial representation and any symmetric group has the alternating representation (which we can verify is irreducible by computing the norm of its character). We can use orthogonality relations to compute the third and final character.

S_3	e	$(1\ 2)$	$(1\ 2\ 3)$
Trivial	1	1	1
Alternating	1	-1	1
Third Rep	2	0	-1

□

0.5 Fall 2014

1. Give definition for each of the following.

   (a) the group S_n,

   Solution. S_n is the group of permutations on the set with n elements under composition. □

   (b) ring,

   Solution. A ring is a set R equipped with two operations $+$ and $\cdot$ such that R is an abelian group under $+$ and that $\cdot$ is associative. □

   (c) ring homomorphism,

   Solution. A ring homomorphism, $\varphi : R \to S$ is a group homomorphism that respects multiplication: $\varphi(ab) = \varphi(a)\varphi(b)$. □

   (d) field,

   Solution. A field is a commutative ring with a multiplicative identity for which every nonzero element has a multiplicative inverse. □

   (e) PID.

   Solution. A principal ideal domain is a ring in which every proper ideal is generated by a single element. □

2. Let F be a field. Prove that $\langle F, +\rangle$ and $\langle F^\times, \cdot\rangle$ are not isomorphic as groups.

Solution. If F is a finite field with q elements then $|F| = q$ and $|F^{\times}| = q - 1$, so the additive and multiplicative groups cannot be isomorphic.

Suppose then that F is not finite. If the characteristic of F is not 2, then the multiplicative group has an element of order 2, -1, whereas the additive group has no such element.

Finally, suppose that F is not finite and has characteristic 2. The equation $x^2 = 1$ has exactly one solution in F, namely 1. However, the corresponding equation $2x = 0$ has every element in F as a solution. Since F contains more than one element, we conclude that these groups are not isomorphic. □

3. True/False. If R is a principal ideal domain and P a nonzero prime ideal of R, then P is a maximal ideal of R.

   Solution. This is true. Suppose (p) is a prime but not maximal ideal of the PID R. Since (p) is not maximal, it is properly contained in a proper maximal ideal (q). We then have that $p = uq$ for some $u \in R$. Since (p) is prime, we then have that u or q is in (p). If $q \in (p)$, then $(q) \subseteq (p)$, which gives $(p) = (q)$, a contradiction. Suppose then that $u \in (p)$. We must then have $u = vp$ for some v. Putting it all together gives

$$p = uq = vpq \implies p(1 - vq) = 0.$$

   Sine R is an integral domain and $p \neq 0$, we must have that $1 = vq$, so q is a unit. But then $(q) = R$, a contradiction. □

4. Prove that no group of order 132 is simple.

   Proof. Suppose G has order $132 = 2^2 \cdot 3 \cdot 11$. By Sylow's theorems, n_3, the number of Sylow 3-subgroups, must be 1 mod 3 and divide 44. We must then have that $n_3 = 1$ or $n_3 = 4$. If $n_3 = 1$, then the lone Sylow 3-subgroup is normal, so suppose that $n_3 = 4$. Again by Sylow's theorem, conjugation induces a transitive action of G on the four Sylow 3-subgroups, i.e. a homomorphism $G \to S_4$. Since $|S_4| < 132$, this homomorphism cannot be injective. Since this action is nontrivial, this homomorphism must have nontrivial kernel: a normal subgroup of G. □

5. Determine the splitting field over $\mathbb{Q}$ of the polynomial $x^4 + x^2 + 1$, and the degree over $\mathbb{Q}$ of the splitting field.

   Solution. Let $p(x) = x^4 + x^2 + 1$. We factor to obtain $p(x) = (x^2 + x + 1)(x^2 - x + 1)$, where both of these quadratics are irreducible over $\mathbb{Q}$ since they have no rational roots. The roots of the first factor are $\frac{-1\pm\sqrt{-3}}{2}$ and the roots of the second are $\frac{1\pm\sqrt{-3}}{2}$.

The extension $\mathbb{Q}(-\sqrt{3})$ definitely contains all roots of $p(x)$, some of which are irrational. Since x^2+3 is irreducible by Eisenstein's criterion, we have that $[\mathbb{Q}(\sqrt{-3}):\mathbb{Q}]=2$, so there is no intermediate extension. We conclude that the splitting field of $p(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{-3})$ and that this extension is quadratic over $\mathbb{Q}$. □

6. Find two 4×4 matrices with the same minimal and characteristic polynomials that are not similar.

   Solution. The matrices with invariant factor lists

   $$\{(x-2),(x-2),(x-2)^2\}, \quad \{(x-2)^2,(x-2)^2\}$$

   are not similar over $\mathbb{Q}$ despite having the same minimal polynomial, $(x-2)^2$, and characteristic polynomial $(x-2)^4$. Two matrices are similar if and only if they have the same rational canonical form if and only if they have the same invariant factor list. The corresponding matrices are similar to

   $$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix} \text{and} \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix},$$

   respectively. □

7. (a) Let R be an integral domain. Prove that $R[x]^\times = R^\times$, i.e., the units in $R[x]$ are the constant polynomials whose constant term is a unit in R.

   Proof. We clearly have the inclusion $R^\times \subseteq R[x]^\times$. Conversely, suppose that $f(x)\in R[x]$ is a unit with inverse $g(x)$. Since R is an integral domain we must have that the degree of $f(x)g(x)=1$ is the sum $\deg f(x)+\deg g(x)$. If $f(x)$ has nonzero degree then we must have that the degree of 1 is nonzero, which is absurd. We must then have that $f(x)$ and $g(x)$ are degree zero, i.e. nonzero constants. But a constant unit is an element of $R^\times$, so we are done. □

   (b) Find an example of a ring R and nonconstant polynomials $f(x),g(x)\in R[x]$ such that $f(x)g(x)=1$.

   Solution. In $(\mathbb{Z}/4\mathbb{Z})[x]$ we have that $(2x+3)^2=1$. □

8. Let p be a prime. Prove that the Galois group for x^p-2 over $\mathbb{Q}$ is isomorphic to the group of matrices

   $$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

   with $a,b\in\mathbb{F}_p$, $a\neq 0$.

Proof. Let $p(x) = x^p - 2$. The roots of this polynomial are $\rho\zeta^k$, where $\rho = 2^{1/p}$, $\zeta = e^{2\pi i/p}$ and $k = 0, 1, \ldots, p-1$. This gives us p distinct complex roots, so $p(x)$ is separable and its splitting field is indeed Galois over $\mathbb{Q}$.

The splitting field of $p(x)$ is clearly contained in $\mathbb{Q}(\rho, \zeta)$. $\mathbb{Q}(\rho)$ isn't big enough since this extension is real and $p(x)$ has non-real roots. This extension has degree p over $\mathbb{Q}$ since ρ has minimal polynomial $x^p - 2$. Similarly, $\mathbb{Q}(\zeta)$ does not contain ρ. This extension has degree $p-1$ over $\mathbb{Q}$ since, by Eisenstein, ζ has minimal polynomial

$$\Phi(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1.$$

The splitting field of $p(x)$ is the smallest extension of $\mathbb{Q}$ containing both ρ and ζ. Since the extensions $\mathbb{Q}(\rho)$ and $\mathbb{Q}(\zeta)$ have relatively prime degrees over $\mathbb{Q}$, the composite extension $\mathbb{Q}(\rho, \zeta)$ has degree $p(p-1)$ over $\mathbb{Q}$.

Now for the Galois group. An automorphism, σ, of $\mathbb{Q}(\rho, \zeta)$ over $\mathbb{Q}$ is determined by where it sends ρ and ζ. σ must also send ρ and ζ to other roots of their respective minimal polynomials. We must then have

$$\sigma(\rho) = \rho\zeta^b, \quad \sigma(\zeta) = \zeta^a,$$

for some $a \in \{1, 2, \ldots, p-1\}$ and $b \in \{0, 1, \ldots, p-1\}$. It's clear that any such σ fixes $\mathbb{Q}$. There are $p-1$ choices for a and p choices for b, so in total we have $p(p-1)$ different maps here. Since the size of the Galois group is the degree of the extension, $p(p-1)$, we have indeed accounted for all maps in the Galois group.

Let Γ be the Galois group of $\mathbb{Q}(\rho, \zeta)$ over $\mathbb{Q}$ and let $\sigma_{a,b}$ be the map that sends ζ to ζ^a and ρ to $\rho\zeta^b$. Call the group of matrices we're interested in G. Define the map $\varphi : \Gamma \to G$ by

$$\sigma_{a,b} \mapsto \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}.$$

The identity map in Γ is $\sigma_{1,0}$, which clearly maps to the identity matrix under φ. Let's compose two elements $\sigma_{a,b}$ and $\sigma_{c,d}$ from Γ.

$$\begin{aligned}(\sigma_{a,b} \circ \sigma_{c,d})(\rho) &= \sigma_{a,b}(\rho\zeta^d) \\ &= \rho\zeta^{ad+b} \\ (\sigma_{a,b} \circ \sigma_{c,d})(\zeta) &= \sigma_{a,b}(\zeta^c) \\ &= \zeta^{ac}.\end{aligned}$$

This gives $\sigma_{a,b} \circ \sigma_{c,d} = \sigma_{ac,ad+b}$. We also have

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix}.$$

Thus, this correspondence is homomorphic. That φ is surjective is clear and injectivity follows from comparing entries, so φ is an isomorphism. □

9. Determine all real matrices with characteristic polynomial $x^3(x^2+1)$ up to conjugation.

Solution. Two matrices are similar over $\mathbb{R}$ if and only if they have the same rational canonical form if and only if they have the same invariant factors. The product of the invariant factors must be $x^3(x^2+1)$ and the minimal polynomial must be divisible by x and x^2+1, as these are the irreducible factors of the characteristic polynomial.

The possible invariant factor lists are then

$$\{x,\ x,\ x(x^2+1)\}, \quad \{x,\ x^2(x^2+1)\}, \quad \{x^3(x^2+1)\}.$$

Taking the direct sum of companion matrices gives these conjugacy classes, respectively.

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

□

10. Suppose p is a prime, and suppose r and N are positive integers. Consider the map $\mathbb{F}_{p^r}^\times \to \mathbb{F}_{p^r}^\times$ that sends x to x^N. What is the cardinality of its kernel and image?

Solution. Let's compute the kernel of this map, which we'll denote by φ, first. Since the multiplicative group of a finite field is cyclic, we can write $\mathbb{F}_{p^r} = \langle g \rangle$. The kernel φ is then the set of g^k such that $Nk \equiv 0 \pmod{p^r - 1}$. This is equivalent to $Nk = m(p^r - 1)$ for some integer m. If we let $\gamma = \gcd(N, p^r - 1)$, then we can divide through by γ to obtain

$$\frac{N}{\gamma} k \equiv 0 \quad (\text{mod } \frac{p^r - 1}{\gamma}).$$

Since N/γ and $(p^r - 1)/\gamma$ are coprime, we can multiply through by the inverse of N/γ to see that $k \equiv 0 \pmod{\frac{p^r-1}{\gamma}}$. The size of $\ker\varphi$ is then the number of multiples of $\frac{p^r-1}{\gamma}$ in $\{0, 1, \dots, p^r - 2\}$, γ.

By the first isomorphism theorem, $\mathbb{F}_{p^r}^\times / \ker\varphi \cong \text{Im } \varphi$, so the image of φ contains $(p^r - 1)/\gamma$ elements. □