

Professor J. Beachy, 9/25/98

1. (20 pts) Prove the Second Isomorphism Theorem. That is, let G be a group, let N be a normal subgroup of G , and let K be any subgroup of G . Prove that $K \cap N$ is a normal subgroup of K , and that KN/N is isomorphic to $K/(K \cap N)$.

Note: You may assume that KN is a subgroup of G .

2. (30 pts) Let G be a group, and let A be a set.

(a) Give the definition of a group action of G on A .

(b) Prove that every group action of G on A determines a group homomorphism from G into the symmetric group S_A .

(c) Assume that $|G| = 36$, and that G has a subgroup H with $|H| = 9$. Explain how G has an action on the set A of left cosets of H , and use this action to show that G must have a proper nontrivial normal subgroup.

3. (35 pts) Let G be a group, and let H be a subgroup of G .

(a) Define the normalizer of H in G .

(b) Recall that a subgroup K of G is called a conjugate of H if $K = gHg^{-1}$, for some $g \in G$. Show that any subgroup conjugate to H is isomorphic to H .

(c) Prove that the conjugates of H are in one-to-one correspondence with the left cosets of the normalizer of H .

(d) Let G be the dihedral group with 12 elements, given by generators a, b with $|a| = 6$, $|b| = 2$, and $ba = a^{-1}b$. Let $H = \{1, a^3, b, a^3b\}$. Find the normalizer of H in G and find the subgroups of G that are conjugate to H .

4. (15 pts) Let a be the cycle $(1, 2, 3)$ in the symmetric group S_5 . Find the centralizer of a in S_5 .

Hint: First determine the order of the centralizer, using the fact that two permutations in S_5 are conjugate if and only if they have the same cycle structure.

EXAM I–Takehome Part

Due Monday, October 5, 1998

Professor J. Beachy, 9/30/98

1. (20 pts) A subgroup H of a finite group G is called a *Hall subgroup* of G if its index in G is relatively prime to its order. That is, if $\gcd(|H|, |G : H|) = 1$. Prove that if H is a Hall subgroup of G and N is any normal subgroup of G , then $H \cap N$ is a Hall subgroup of N and HN/N is a Hall subgroup of G/N .
2. (30 pts) Let G be a group, and let A be a set. In your own words, write out proofs of the following results.
 - (a) Prove that every group action of G on A determines a group homomorphism from G into the symmetric group S_A .
 - (b) Let H be a subgroup of G . Explain how G has an action on the set A of left cosets of H . Use this action to show that if H has index n , then G must have a proper nontrivial normal subgroup whose index is a divisor of $n!$.
3. (30 pts) Let G be a group, and let H be a subgroup of G .
 - (a) Prove that the subgroups conjugate to H are in one-to-one correspondence with the left cosets of the normalizer of H . You should give two proofs: one that uses group actions and one that is direct.
 - (b) Let G be the dihedral group with 12 elements, given by generators a, b with $|a| = 6$, $|b| = 2$, and $ba = a^{-1}b$. For each proper nontrivial subgroup of G , find all conjugate subgroups.
4. (20 pts) Find the centralizer of $(1, 2, 3)$ in the symmetric group S_n , for all $n \geq 3$.

Each problem is worth 20 points.

1. (a) Write out the class equation for a finite group G , and define each term.
(b) State and prove the first Sylow theorem.
2. Prove that there are no simple groups of order 96 or 135.
3. For the special case of an abelian group G of order 72, write out the proof that G is isomorphic to a direct product of its Sylow subgroups.
4. Let G be a group of order p^2q^2 , where p and q are distinct primes.
 - (a) Given that G is abelian, what are the possibilities for its structure?
 - (b) Show that if G has a unique Sylow p -subgroup and a unique Sylow q -subgroup, then G is abelian.
5. Let G be the group of matrices of the form $\begin{bmatrix} 1 & 0 \\ x & a \end{bmatrix}$ such that $x \in \mathbf{Z}_7$ and $a \in \mathbf{Z}_7^\times$.
 - (a) Find (list the elements) a Sylow 7-subgroup of G . Find the number of Sylow 7-subgroups of G .
 - (b) Find a Sylow 3-subgroup of G . Find the number of Sylow 3-subgroups of G .

The test is due at 5:00 p.m. on Monday, November 23.

1. (13.2 #18) Let F be a field, and let $F(x)$ be the field of rational functions in x with coefficients from F . Let $P(x), Q(x) \in F[x]$ be relatively prime, with $Q(x) \neq 0$, and let $t = P(x)/Q(x)$.
 - (a) Show that $P(X) - tQ(X) \in (F(t))[X]$ is irreducible over $F(t)$ and has x as a root.
 - (b) Show that $\deg(P(X) - tQ(X)) = m$, where $m = \max(\deg(P(x)), \deg(Q(x)))$.
 - (c) Show that $[F(x) : F(t)] = m$.
2. (13.5 #5) Prove that if p is prime and $a \neq 0$, then $x^p - x + a$ is irreducible over \mathbf{Z}_p .
3. (13.5 #10) Let $f(x_1, x_2, \dots, x_n) \in \mathbf{Z}[x_1, x_2, \dots, x_n]$. Prove that in $\mathbf{Z}_p[x_1, x_2, \dots, x_n]$ we have $(f(x_1, x_2, \dots, x_n))^p = f(x_1^p, x_2^p, \dots, x_n^p)$.
4. (13.6 #5) Prove that if $n > 1$ is odd, then $\Phi_{2n}(x) = \Phi_n(-x)$.
5. (13.6 #10) Let ϕ be the Frobenius mapping $\phi(x) = x^p$ on the finite field $GF(p^n)$. Prove that ϕ is an automorphism with order n .
6. (14.1 #7) Show that $\text{Aut}(\mathbf{R}/\mathbf{Q})$ is trivial.
7. (14.1 #8) Prove that the automorphisms of $F(x)$ that fix F are precisely the fractional linear transformations determined by $\theta(x) = \frac{ax + b}{cx + d}$, where $a, b, c, d \in F$ with $ad - bc \neq 0$.
8. (14.1 #10) Let K be an extension of the field F . Let $\phi : K \rightarrow K'$ be an isomorphism of K that maps F to F' . Prove that $\sigma \mapsto \phi\sigma\phi^{-1}$ defines an isomorphism from $\text{Aut}(K/F)$ onto $\text{Aut}(K'/F')$.

Each question is worth 25 points.

1. State and prove *either* the Second Isomorphism Theorem *or* the Third Isomorphism Theorem.
2. (a) Write out the conjugacy class equation for a finite group, and define each term.
(b) Use the conjugacy class equation to prove that any p -group has a nontrivial center.
3. (a) State the Sylow theorems.
(b) Prove that a group of order 48 must have a normal subgroup of order 8 or 16.
4. (a) State the fundamental structure theorem for finite abelian groups.
(b) Let G be an abelian group with 243 elements. Assume that G has elements of order 9, but none of higher order. How many elements of order 9 must it have?
5. (a) Define: algebraic element in an extension field; algebraic extension.
(b) Prove that if $K \subseteq E \subseteq F$ are fields such that E is an algebraic extension of K and F is an algebraic extension of E , then F is an algebraic extension of K .
6. (a) Let F be a splitting field for $f(x) \in K[x]$. Define $\text{Gal}(F/K)$.
(b) Find the Galois group of the polynomial $x^5 - 1$ over \mathbf{Q} .
7. (a) State the fundamental theorem of Galois theory.
(b) Let F be a splitting field for $f(x) \in K[x]$, and let E be an intermediate field with $K \subseteq E \subseteq F$. If $\text{Gal}(F/K) = S_3$ and E is a splitting field over K with $E \neq K$, what can you say about $[E : K]$?
8. Let p be a prime number, and let F be a field with $q = p^n$ elements, where $n > 1$.
(a) Prove that F is the splitting field of $x^q - x$ over its prime subfield \mathbf{Z}_p .
(b) Prove that $\text{Gal}(F/\mathbf{Z}_p)$ is a cyclic group.

Take-home part

1. (20 pts) A subgroup H of a finite group G is called a *Hall subgroup* of G if its index in G is relatively prime to its order. That is, if $\gcd(|H|, |G : H|) = 1$. Prove that if H is a Hall subgroup of G and N is any normal subgroup of G , then (a) $H \cap N$ is a Hall subgroup of N and (b) HN/N is a Hall subgroup of G/N .

Solution. Assume that $|H|$ is relatively prime to $|G : H|$. We will use the fact that any divisor of $|H|$ must be relatively prime to any divisor of $|G : H|$. We also need to use the second isomorphism theorem, which states that HN/N is isomorphic to $H/H \cap N$, so

$$\frac{|HN|}{|N|} = \frac{|H|}{|H \cap N|} \quad \text{or} \quad \frac{|HN|}{|H|} = \frac{|N|}{|H \cap N|}.$$

To prove part (a) we have the following computations.

$$|H \cap N| \cdot |H : H \cap N| = |H|$$

$$|N : H \cap N| \cdot |G : HN| = \frac{|N|}{|H \cap N|} \cdot \frac{|G|}{|HN|} = \frac{|HN|}{|H|} \cdot \frac{|G|}{|HN|} = \frac{|G|}{|H|} = |G : H|$$

To prove part (b) we have the following computations.

$$|HN/N| \cdot |H \cap N| = \frac{|HN|}{|N|} \cdot |H \cap N| = \frac{|H|}{|H \cap N|} \cdot |H \cap N| = |H|$$

$$|G/N : HN/N| \cdot |HN : H| = \frac{|G|}{|N|} \cdot \frac{|N|}{|HN|} \cdot \frac{|HN|}{|H|} = \frac{|G|}{|H|} = |G : H|$$

2. (30 pts) Let G be a group, and let A be a set. In your own words, write out proofs of the following results.

(a) Prove that every group action of G on A determines a group homomorphism from G into the symmetric group S_A .

Solution. Assuming that G acts on A , for each $g \in G$ define $\lambda_g : A \rightarrow A$ by $\lambda_g(a) = g \cdot a$, for all $a \in A$. An easy computation establishes the formula $\lambda_g \lambda_h = \lambda_{gh}$, for all $g, h \in G$. It follows that $\lambda_{g^{-1}} = \lambda_g^{-1}$, so λ_g is a permutation of A . The above formula also shows that defining $\Phi : G \rightarrow S_A$ by $\Phi(g) = \lambda_g$, for all $g \in G$, gives the required group homomorphism.

(b) Let H be a subgroup of G . Explain how G has an action on the set A of left cosets of H . Use this action to show that if H is a proper subgroup with index n , then G must have a proper normal subgroup whose index is a divisor of $n!$.

Solution. Define the group action from $G \times A$ into A by $g \cdot aH = (ga)H$, for all $g, a \in G$. Since $1 \cdot aH = aH$ and $(gh) \cdot aH = (gh)aH = g(ha)H = g \cdot (h \cdot aH)$, we have in fact defined a group action. If $|G : H| = n$, then we can identify S_A with S_n , so the homomorphism Φ defined by the group action maps G into S_n . If H is a proper subgroup, and $g \in G \setminus H$, then $\Phi(g) \neq 1$, so $\ker(\Phi)$ is a proper normal subgroup of G . Since $G/\ker(\Phi)$ is isomorphic to a subgroup of S_n , it follows that $|G : \ker(\Phi)|$ is a divisor of $|S_n| = n!$.

3. (30 pts) Let G be a group, and let H be a subgroup of G .

(a) Prove that the subgroups conjugate to H are in one-to-one correspondence with the left cosets of the normalizer of H . You should give two proofs: one that uses group actions and one that is direct.

First Solution. Let A be the set of all subgroups conjugate to H , so that $A = \{aHa^{-1} \mid a \in G\}$. We can define a group action of G on A by setting $g * aHa^{-1} = (ga)H(ga)^{-1}$. This is indeed a group action since $1 * aHa^{-1} = aHa^{-1}$ and $gk * aHa^{-1} = ((gk)a)H((gk)a)^{-1} = (g(ka))H(g(ka))^{-1} = g((ka)H(ka)^{-1})g^{-1} = g * (k * aHa^{-1})$, for all $g, k \in G$. The orbit of H under this action gives all of A . From our general results, elements in the orbit of H are in one-to-one correspondence with left cosets of the stabilizer of H , which is $\{g \in G \mid gHg^{-1} = H\} = N_G(H)$.

Second Solution. For $g, k \in G$, we have $gHg^{-1} = kHk^{-1}$ if and only if $k^{-1}gHg^{-1}k = H$, which occurs if and only if $k^{-1}g \in N_G(H)$, and this happens if and only if $gN_G(H) = kN_G(H)$. Thus g and k determine the same conjugate of H if and only if they belong to the same left coset of the normalizer $N_G(H)$. This shows that the conjugates of H can be put in one-to-one correspondence with the left cosets of $N_G(H)$. To complete the proof, define $\Phi(gN_G(H)) = gHg^{-1}$, and show that Φ is well-defined, one-to-one, and onto.

(b) Let G be the dihedral group with 12 elements, given by generators a, b with $|a| = 6$, $|b| = 2$, and $ba = a^{-1}b$. For each proper nontrivial subgroup of G , find all conjugate subgroups.

Solution. The subgroups of G are as follows.

order 6: $\langle a \rangle$, $\{1, a^2, a^4, b, a^2b, a^4b\}$, $\{1, a^2, a^4, ab, a^3b, a^5b\}$. The subgroups of order 6 are normal since they have order $|G|/2$, so they have no conjugates.

order 4: There are three subgroups of order 4, and they are conjugate, as shown in the solution (given below) to question 3 (d) of the in-class test.

order 3: $\{1, a^2, a^4\}$. This subgroup is normal (it is a union of conjugacy classes).

order 2: $\{1, a^3\}$, $\{1, b\}$, $\{1, a^2b\}$, $\{1, a^4b\}$, $\{1, ab\}$, $\{1, a^3b\}$, $\{1, a^5b\}$. The first subgroup is the center, which is normal. The next three are conjugate, since we only need to worry about conjugacy of elements. The last three are also conjugate.

For example, the normalizer of $H = \{1, b\}$ includes at least the subgroup and the center of G . The first computation (with a) shows that $N_G(H) = \{1, b, a^3, a^3b\}$, with left cosets represented by $1, a$, and a^2 .

$$a\{1, b\}a^{-1} = \{1, a^2b\}$$

$$a^2\{1, b\}a^{-2} = \{1, a^4b\}$$

3. (20 pts) Find the centralizer of $(1, 2, 3)$ in the symmetric group S_n , for all $n \geq 3$.

Solution. There are $n(n-1)(n-2)/3$ three-cycles in S_n , and these are the conjugates of $(1, 2, 3)$, so the centralizer of $(1, 2, 3)$ must have $3(n-3)!$ elements. These can be found by multiplying a power of $(1, 2, 3)$ by any permutation that is disjoint from $(1, 2, 3)$.

In-class part

2. (c) Assume that $|G| = 36$, and the G has a subgroup H with $|H| = 9$. (We now know that G has to have such a subgroup, since G must have a Sylow 3-subgroup.) The index of H in G is 4, so letting G act by multiplication on the left cosets of H produces a group homomorphism from G into S_4 . The kernel of this homomorphism is a proper normal subgroup, and it cannot be trivial since 36 is not a divisor of $4! = 24$.

3. (d) Let G be the dihedral group with 12 elements, given by generators a, b with $|a| = 6$, $|b| = 2$, and $ba = a^{-1}b$. Let $H = \{1, a^3, b, a^3b\}$. Find the normalizer of H in G and find the subgroups of G that are conjugate to H .

Solution. The normalizer of H is a subgroup containing H , so since H has index 3, either $N_G(H) = H$ or $N_G(H) = G$. Choose any element not in H to do the first conjugation.

$$aHa^{-1} = \{1, a(a^3)a^5, aba^5, a(a^3b)a^5\} = \{1, a^3, a^2b, a^5b\}$$

This computation shows that a is not in the normalizer, so $N_G(H) = H$. Furthermore, conjugating by any element in the same left coset $aH = \{a, a^4, ab, a^4b\}$ will give the same subgroup. Therefore it makes sense to choose a^2 to do the next computation.

$$a^2Ha^{-2} = \{1, a^3, a^2ba^4, a^2(a^3b)a^4\} = \{1, a^3, a^4b, ab\}$$

It is interesting to note that we had shown earlier that a^2b and a^4b are conjugate to b , while ab , a^3b , and a^5b are conjugate. The above computations show how the orbits of individual elements combine to give the orbit of a subgroup.

Some of these problems are interesting but not central to Galois theory. I have changed the order to put the most important ones first. The “solutions” are just outlined.

1. (13.6 #10) Let ϕ be the Frobenius mapping $\phi(x) = x^p$ on the finite field $GF(p^n)$. Prove that ϕ is an automorphism with order n .

Soln: See Corollary 8.1.7 in Beachy and Blair.

2. (14.1 #10) Let K be an extension of the field F . Let $\phi : K \rightarrow K'$ be an isomorphism of K that maps F to F' . Prove that $\sigma \mapsto \phi\sigma\phi^{-1}$ defines an isomorphism from $\text{Aut}(K/F)$ onto $\text{Aut}(K'/F')$.

Soln: Define $\Phi(\sigma) = \phi\sigma\phi^{-1}$. The first task is to show that $\Phi(\sigma) \in \text{Aut}(K'/F')$. Since ϕ and σ are automorphisms, so is $\Phi(\sigma)$. It must also be checked that $\phi\sigma\phi^{-1}(x) = x$ for all $x \in F'$. This follows from the fact that elements of F' correspond to those in F , which are fixed by σ . There is an obvious inverse function $\Phi^{-1}(\tau) = \phi^{-1}\tau\phi$, and so Φ is one-to-one and onto. Finally, it is necessary to show that Φ preserves addition and multiplication, but these facts follow immediately.

3. (13.5 #5) Prove that if p is prime and $a \neq 0$, then $f(x) = x^p - x + a$ is irreducible over \mathbf{Z}_p .

Soln: If c is a root and $m \in \mathbf{Z}_p$, then $c + m$ is also a root, since $f(c + m) = (c + m)^p - (c + m) + a = c^p + m^p - c - m + a = (c^p - c + a) + (m^p - m) = 0 + 0$. (We have $m^p - m = 0$ in \mathbf{Z}_p .)

Suppose that $f(x)$ is reducible and factors as $g(x)h(x)$ over \mathbf{Z}_p , where $g(x)$ has degree $d < p$. If we adjoin a root of $f(x)$, then we get a splitting field (by the previous paragraph). In this field $g(x) = \prod_{i=1}^d (x - (c + m_i))$, and

expanding this we see that the coefficient b_{d-1} of x^{d-1} in $g(x)$ has the form $-\sum_{i=1}^d (c+m_i) = -dc - \sum_{i=1}^d m_i = -dc + k$, for some $k \in \mathbf{Z}_p$. By assumption this coefficient is in \mathbf{Z}_p , so we can solve for c since d is invertible in \mathbf{Z}_p . Therefore $c \in \mathbf{Z}_p$, a contradiction.

4. (13.5 #10) Let $f(x_1, x_2, \dots, x_n) \in \mathbf{Z}[x_1, x_2, \dots, x_n]$. Prove that in $\mathbf{Z}_p[x_1, x_2, \dots, x_n]$ we have

$$(f(x_1, x_2, \dots, x_n))^p = f(x_1^p, x_2^p, \dots, x_n^p).$$

Soln: For the case of one variable we have $(f(x))^p = (\sum_{i=1}^m a_i x^i)^p = \sum_{i=1}^m (a_i x^i)^p = \sum_{i=1}^m a_i^p (x^i)^p = \sum_{i=1}^m a_i (x^p)^i = f(x^p)$. We can use induction to complete the proof, since a polynomial in n indeterminates can be written in the form $f(x_1, \dots, x_{n-1}, x_n) = \sum_{i=1}^m a_i(x_1, \dots, x_{n-1})x_n^i$ by thinking of it as an element of the polynomial ring $F(x_1, \dots, x_{n-1})[x_n]$.

5. (13.6 #5) Prove that if $n > 1$ is odd, then $\Phi_{2n}(x) = \Phi_n(-x)$.

Soln: One proof uses induction. For $n = 2q$ we have $x^n - 1 = (x^q)^2 - 1 = (x^q - 1)(x^q + 1)$. Then $x^q - 1 = \prod_{d|q} \Phi_d(x)$ and $x^q + 1 = -((-x)^q - 1) = -\theta(x^q - 1) = (-1)\theta(\prod_{d|q} \Phi_d(x)) = (-1)(-\Phi_2(x))(\prod_{d|q, d \neq 1} \Phi_d(-x)) = \Phi_2(x) \prod_{d|q, d \neq 1} \Phi_d(-x)$. If d is an odd divisor of n , then $\Phi_d(x)$ occurs as an irreducible factor of $x^q - 1$. Therefore if d is an even divisor of n , then $\Phi_d(x)$ occurs as an irreducible factor of $x^q + 1$. By the induction hypothesis, if $d = 2s$ is an even divisor of n , with $2 < d < 2q$, then $\Phi_d(x) = \Phi_s(-x)$. Together with $\Phi_2(x)$, this accounts for all of the irreducible factors of $x^q + 1$ except $\Phi_{2q}(x)$, and so it follows from the unique factorization theorem for polynomials that $\Phi_{2q}(x) = \pm \Phi_q(-x)$. The degree of $\Phi_q(x)$ is even, so in fact we must have $\Phi_{2q}(x) = \Phi_q(-x)$.

A second proof can be given by showing that defining $f(\omega) = -\omega$ gives a one-to-one correspondence between the primitive n th roots of unity and the primitive $2n$ th roots of unity. This works because of some elementary group theory: if n is odd and ω has order n , then $-\omega = (-1)\omega$ and -1 has order 2, which is relatively prime to n . It follows that $-\omega$ has order $2n$. The function f is clearly one-to-one, and it is onto since both sets have the same number of elements. (For the Euler φ -function, $\varphi(2n) = \varphi(2)\varphi(n)$ since $\gcd(2, n) = 1$, and $\varphi(2) = 1$, so $\varphi(2n) = \varphi(n)$.)

6. (14.1 #7) Show that $\text{Aut}(\mathbf{R}/\mathbf{Q})$ is trivial.

Soln: I think that the hints given by Dummit and Foote are quite transparent.

7. (13.2 #18) Let F be a field, and let $F(x)$ be the field of rational functions in x with coefficients from F . Let $P(x), Q(x) \in F[x]$ be relatively prime, with $Q(x) \neq 0$, and let $t = P(x)/Q(x)$.

(a) Show that $P(X) - tQ(X) \in (F(t))[X]$ is irreducible over $F(t)$ and has x as a root.

(b) Show that $\deg(P(X) - tQ(X)) = m$, where $m = \max(\deg(P(x)), \deg(Q(x)))$.

(c) Show that $[F(x) : F(t)] = m$.

Soln: My proof pretty much follows the hints given by Dummit and Foote. You have to be careful in using Gauss's lemma. In fact, you need Corollary 6 on page 299, where it is required that the gcd of the coefficients must be 1. This is where you need the assumption that $P(x)$ and $Q(x)$ are relatively prime. Then considering $P(X) - tQ(X)$ as an element of $(F[X])[t]$ gives the irreducibility. The rest of the proof follows quickly.

8. (14.1 #8) Prove that the automorphisms of $F(x)$ that fix F are precisely the fractional linear transformations determined by $\theta(x) = \frac{ax+b}{cx+d}$, where $a, b, c, d \in F$ with $ad - bc \neq 0$.

Soln: Let θ be any automorphism of $F(x)$ that fixes F . Then the image $\theta(x)$ of x is some element of $F(x)$, which we can write in the form $\theta(x) = \frac{P(x)}{Q(x)} = t$. The image of θ is in $F(x)$ is $F(t)$, and since θ is an automorphism, we must have $[F(x) : F(t)] = 1$. Therefore we can apply the previous problem to show that $P(x)$ and $Q(x)$ must have degree 1 and be relatively prime. Note that $ax + b$ and $cx + d$ are relatively prime if and only if $x + b/a \neq x + d/c$, or $b/a \neq d/c$. This translates into the condition that $bc \neq ad$.