MATH 3320, SPRING 2012:
ANSWERS TO THE QUIZZES

PR HEWITT

Quiz 1: 11 January

(1) What is an algorithm?
An algorithm is a finite, step-by-step procedure for solving a problem.
(2) What are special properties of conjugation in a quadratic extension?
Conjugation is an isomorphism of the field, meaning that it is a bijection which respects sum and product.
(3) Is trisecting an angle impossible?
It is possible using the right tools. It is impossible using only straightedge and compass.
(4) Why did Galois introduce the concept of a group?
A group is an algebraic measure of symmetry, which Galois used to explain why some polynomial equations are solvable by elementary means while others are not.
(5) What is the trend in algebra over the last two centuries?
Since the time of Galois algebra has become increasingly concerned with abstract structure rather than algorithms. There has been a renewed interest in algorithms with the advent of electronic computers.

Quiz 2: 18 January

(1) What profound effect did the search for an algorithmic solution of quintic equations have on the history of algebra?
Galois invented the abstract structure of a group in order to explain the Abel-Ruffini theorem that such a solution is impossible. From about this time forward algebra turned increasingly from a search for algorithms to a study of abstract structure.
(2) What is the main point of chapter 1 in our text? How is this illustrated?
The main point of chapter 1 is to show how an understanding of the symmetries of a figure must examine the algebraic structure of the composition of symmetries. This is illustrated by a close comparison of the algebraic properties of the groups of the tetrahedron and of the hexagon.
(3) How many nonidentity rotations of the tetrahedron equal their inverse?
There are three such rotations. Each is the rotation through an angle of π around an axis joining the midpoints of a pair of opposite edges.

Date: 23 April 2012.

(4) Is there a nonidentity rotation of the tetrahedron that commutes with all other rotations of the tetrahedron?

No. In fact none of the rotations described above commute with any of the nonidentity rotations around an axis passing through a vertex and the centroid of its opposite face.

(5) Is there a nonidentity symmetry of the hexagon that commutes with all other symmetries of the hexagon ?

Yes, there is exactly one — namely the rotation through an angle π around the axis perpendicular to the hexagon and passing through its centroid.

Quiz 3: 25 January

(1) What is the definition of a group? *Be precise!*

A group is set G together with a multiplication $G \times G \to G$ satisfying three simple axioms. (Note: We denote the image of the pair (x, y) under multiplication by xy.)

- The multiplication is associative: that is, for all $x, y, z \in G$ we have $(xy)z = x(yz)$.
- There is an identity element $e \in G$: that is, for all $x \in G$ we have $xe = ex = x$.
- Every element G has an inverse in G: that is, for all $x \in G$ there is an element $y \in G$ such that $xy = yx = e$.

(2) State and prove one of the two lemmas from chapter 2.

One of the lemmas stated that in a group G the identity element is unique. In other words, if e and f are both identity elements in G then $e = f$. *Proof:* Since e is an identity we have that $ef = f$. Since f is an identity we have that $ef = e$. Hence $e = ef = f$.

The second lemma says that if x is an element of the group G then its inverse is unique. It can be proved in a similar way: if y and z are both inverses for x then $y = y(xz) = (yx)z = z$.

Quiz 4: 30 January

(1) What is $5 \times 3 \bmod 7$?

$5 \times 3 = 15 = 2 \times 7 + 1 \equiv 1 \bmod 7$

(2) What is the additive inverse of 8 in $\mathbb{Z}_{23}$?

If x is the additive inverse of then $8 + x \equiv 0 \bmod 23$. That is, $23 \mid 8 + x$. Since $8 + 15 = 23$ we find that $x = -8 \equiv 15 \bmod 23$.

(3) Does 8 have a multiplicative inverse in $\mathbb{Z}_{23} - \{0\}$?

If x were the additive inverse of then $8x \equiv 1 \bmod 23$. That is, $23 \mid 8x - 1$. Since $8 \times 3 - 1 = 23$ we find that 3 is a multiplicative inverse for 8 mod 23.

(4) Is $\mathbb{Z}_6 - \{0\}$ a group under multiplication modulo 6?

No. It is not even closed under multiplication, for example $2 \times 3 = 6 \equiv 0 \bmod 6$.

(5) Is $\{z \in \mathbb{Z} \mid z > 0\}$ a group under multiplication?

No. Interestingly it is closed and associative under multiplication, has a multiplicative identity — namely 1 — and satisfies the cancellation laws. However no positive integer except 1 has a multiplicative inverse amongst the positive integers.

Quiz 5: 10 February

(1) What is the dihedral group D_n?

The dihedral group D_n is the group of symmetries of a regular n-gon.

(2) What is the order of D_n?

D_n has exactly $2n$ symmetries: the identity; $n-1$ nonidentity rotations; and n reflections.

(3) How many elements of D_n have order 2?

If n is odd then D_n has exactly n elements of order 2 — namely the n reflections. If n is even then in addition to the n reflections there is one additional element of order 2 — namely the rotation through angle π.

(4) Give two examples of groups of order 12.

There are many many such groups: for example all three groups from chapter 1 have order 12.

(5) Give an example of a group of infinite order.

There are many many such groups: for example, the additive groups $\mathbb{Z}$ and $\mathbb{R}$; the unit circle C; the Lorentz group.

Quiz 6: 20 February

(1) What was the historical impetus for first studying groups?

Groups were first defined by Évariste Galois in the early 19th century. He used them to explain which equations can be solved "by radicals" and which cannot.

(2) Let s be a reflection in the dihedral group D_n. Which elements of D_n commute with s?

If r is the rotation counterclockwise thru angle $2\pi/n$ then $sr^k = r^{n-k}s$. Every element of D_n has the form r^k or sr^k. Thus if n is odd then s commutes only with e and itself. However if n is even then s also commutes with $r^{n/2}$ and $sr^{n/2}$.

(3) Which elements of $\mathbb{Z}_{15}$ have a multiplicative inverse?

If $x \in \mathbb{Z}_{15}$ then $y \bmod 15$ is a multiplicative inverse for x if and only if there is an integer k such that $xy + 15k = 1$. There is such a y if and only if $\gcd(x, 15) = 1$. In other words the elements of $\mathbb{Z}_{15}$ that have multiplicative inverses are precisely those not divisible by either 3 or 5, namely the eight elements 1, 2, 4, 7, 8, 11, 13, and 14.

(4) Which elements of $\mathbb{Z}_{15}$ are generators for the additive group?

Miraculously (or not) the answer to this question is the same as the answer to the previous question. The reason is that x is a generator of the additive group $\mathbb{Z}_{15}$ if and only if 15 is the smallest positive k such $15 \mid kx$. This happens precisely when neither 3 nor 5 divides x.

(5) Write the permutation $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 4 & 6 & 3 \end{bmatrix}$ as a product of disjoint cycles.

Let f be the permutation above. We see that $f(1) = 2$ and $f(2) = 1$, so the first cycle in the product is (12). Next, $f(3) = 5$, $f(5) = 6$, and $f(6) = 3$, so the second cycle in the product is (365). Since f fixes the only remaining point 4, we conclude that $f = (12)(365)$.

Quiz 7: 2 March

Suppose that G and H are groups and that $\varphi\colon G \to H$ is an isomorphism. Prove two of the following statements.

(1) If e is the identity element of G then $\varphi(e)$ is the identity element of H.

Let e' denote the identity element of H. From $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$ we find that $e' = \varphi(e)^{-1}\varphi(e) = \varphi(e)^{-1}\varphi(e)\varphi(e) = \varphi(e)$.

(2) If $x \in G$ then $\varphi(x^{-1}) = \varphi(x)^{-1}$.

We apply the result above. From $e' = \varphi(e) = \varphi(x^{-1})\varphi(x)$ we find that $\varphi(x)^{-1} = e'\varphi(x)^{-1} = \varphi(x^{-1})\varphi(x)\varphi(x)^{-1} = \varphi(x^{-1})$.

(3) If G is cyclic then so is H.

Suppose that $G = \langle x \rangle$. I claim that $H = \langle \varphi(x) \rangle$. Let $y \in H$. Since φ is a bijection there is a $z \in G$ such that $\varphi(z) = y$. By assumption there is an integer m such that $z = x^m$. Hence $y = \varphi(x^m) = \varphi(x)^m$, as required.

(4) If G is abelian then so is H.

Let $y, z \in H$. Since φ is a bijection there are $w, x \in G$ such that $\varphi(w) = y$ and $\varphi(x) = z$. Since G is abelian we find that $yz = \varphi(w)\varphi(x) = \varphi(wx) = \varphi(xw) = \varphi(x)\varphi(y) = zy$, as required.

(5) The function $\varphi^{-1}\colon H \to G$ is an isomorphism.

φ^{-1} is a bijection with inverse φ. We must show that φ^{-1} preserves multiplication. Let $y, z \in H$. Since φ is a bijection there are unique $w, x \in G$ such that $\varphi(w) = y$ and $\varphi(x) = z$. Hence $\varphi^{-1}(y) = w$ and $\varphi^{-1}(z) = x$. Since $\varphi(wx) = \varphi(w)\varphi(x) = yz$ we conclude that $wx = \varphi^{-1}(yz)$. Thus $\varphi^{-1}(y)\varphi^{-1}(z) = wx = \varphi^{-1}(yz)$, as required.

Quiz 8: 14 March

(1) For each platonic solid S let $G(S)$ denote the group of rotations of S. Fill in each of the following blanks with either A_4, S_4, A_5, or S_5. (Recall that $\cong$ means "is isomorphic to".)

$$\begin{array}{rcc} G(\text{tetrahedron}) & \cong & \underline{\quad A_4 \quad} \\ G(\text{hexahedron}) & \cong & \underline{\quad S_4 \quad} \\ G(\text{octahedron}) & \cong & \underline{\quad S_4 \quad} \\ G(\text{dodecahedron}) & \cong & \underline{\quad A_5 \quad} \\ G(\text{icosahedron}) & \cong & \underline{\quad A_5 \quad} \end{array}$$

(2) For at least two of the above describe the isomorphism explicitly.

If we enumerate the four vertices of the tetrahedron then the permutation action on these four provides a map $\varphi\colon G(\text{tetrahedron}) \to S_4$, which one can prove provides an isomorphism between the rotation group and A_4.

If we enumerate the four long diagonals of the hexahedron then the permutation action on these four provides a map $\varphi\colon G(\text{hexahedron}) \to S_4$, which one can prove is an isomorphism.

Since the octahedron is dual to the hexahedron is has the same group of rotations. Hence one way to construct an isomorphism $\varphi\colon G(\text{octahedron}) \to S_4$ is to compose the isomorphisms $G(\text{octahedron}) \to G(\text{dodecahedron})$ and $G(\text{octahedron}) \to S_4$.

Each diagonal of a given face of a dodecahedron is an edge of a unique inscribed hexahedron. Thus there are five such inscribed hexahedra, and if we enumerate these then the permutation action on them provides a map $\varphi\colon G(\text{dodecahedron}) \to S_5$, which one can prove provides an isomorphism between the rotation group and A_5.

Since the octahedron is dual to the hexahedron is has the same group of rotations. Hence one way to construct an isomorphism $\varphi\colon G(\text{octahedron}) \to A_5$ is to compose the isomorphisms $G(\text{octahedron}) \to G(\text{dodecahedron})$ and $G(\text{octahedron}) \to A_5$.

Quiz 9: 16 March

(1) What is A^t?
A^t is the transpose of A. If the ij-entry of A is a_{ij} then the ij-entry of A^t is a_{ji}.
(2) What is an orthogonal matrix?
A square matrix A is orthogonal if and only if $A^tA = I$ (the identity matrix).
(3) What is GL_n?
GL_n is the set of $n \times n$ invertible matrices with real entries.
(4) What is O_n?
$O_n = \{A \in GL_n \mid A^tA = I\}$.
(5) What is SO_n?
$SO_n = \{A \in O_n \mid \det(A) = 1\}$.

Quiz 10: 28 March

For each of the following answer 'true' or 'false':

(1) If H and K are abelian then so is $H \times K$.
True: if H and K are abelian then for any $h_1, h_2 \in H$ and $k_1, k_2 \in K$
$(h_1, k_1) \cdot (h_2, k_2) = (h_1h2, k_1k_2) = (h_2h1, k_2k_1) = (h_2, k_2) \cdot (h_1, k_1)$.
(2) If $H \times K$ is abelian then so are H and K.
True: H and K are isomorphic to subgroups of $H \times K$, and any subgroup of an abelian group is abelian.
(3) If H and K are cyclic then so is $H \times K$.
False: $\mathbb{Z}$ is cyclic but $\mathbb{Z} \times \mathbb{Z}$ is not.
(4) If $H \times K$ is cyclic then so are H and K.
True: H and K are isomorphic to subgroups of $H \times K$, and any subgroup of a cyclic group is cyclic.
(5) If H and K are finite then $|H \times K| = |H| \cdot |K|$.
True.

Quiz 11: 2 April

Let G be a group and H a subgroup. Define a relation $\mathcal{R}$ on G by setting $x\mathcal{R}y$ when $x^{-1}y \in H$.

(1) Prove that $\sim$ is an equivalence relation.

Reflexivity: If $x \in G$ then $x^{-1}x = e \in H$. Hence $x\mathcal{R}x$.

Symmetry: If $x, y \in G$ and $x\mathcal{R}y$ then $x^{-1}y \in H$, whence $y^{-1}x = (x^{-1}y)^{-1} \in H$. Thus $y\mathcal{R}x$.

Transitivity: If $x, y, z \in G$ and $x\mathcal{R}y\mathcal{R}z$ then $x^{-1}y \in H$ and $y^{-1}z \in H$, whence $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$. Thus $x\mathcal{R}z$.

(2) Describe the equivalence classes.

If $x \in G$ then its equivalence class $\mathcal{R}(x)$ is defined to be

$$\{y \in G \mid x\mathcal{R}y\}.$$

If $x\mathcal{R}y$ then the element $h = x^{-1}y \in H$, and conversely. Equivalently $y = xh$ for some $h \in H$. In other words, $\mathcal{R}(x)$ is simply the coset xH.

Quiz 12: 6 April

Use Lagrange's Theorem to prove two of the following three propositions.

(1) If G is a finite group of order n and $x \in G$ then $x^n = e$.

Let $H = \langle x \rangle$ and set $m = |x|$. Note that also $m = |H|$. By Lagrange's Theorem $n = mk$ for some integer k. Hence $x^n = (x^m)^k = e^k = e$.

(2) If G is a finite group of prime order p then G is cyclic.

Suppose $x \in G - \{e\}$. Let $H = \langle x \rangle$ and set $m = |H|$. Since $x \neq e$ we know that $m > 1$. By Lagrange 's Theorem m divides p. Hence $m = p$ and $H = G$.

(3) If n is a positive integer and p is a prime that does not divide n then $n^{p-1} \equiv 1 \bmod p$.

Let r be the remainder of $n \bmod p$. Thus r is in the multiplicative group $\mathbb{Z}_p - \{0\}$ of order $p - 1$. Moreover $r^k \equiv n^k$ for every positive k. By the corollary to Lagrange's Theorem (part (1) above) $n^{p-1} \equiv r^{p-1} \equiv 1 \bmod p$.

Quiz 13: 11 April

(1) Suppose that G is an abelian group of order 30. Use Cauchy's Theorem to prove that G is cyclic.

A corollary to Cauchy's Theorem tells us that there exist a, b, c in G of orders 2, 3, and 5, respectively. Since 2 and 3 are relatively prime and a and b commute we find that $|ab| = 2 \cdot 3 = 6$. Since 6 and 5 are relatively prime and ab and c commute we find that $|abc| = 6 \cdot 5 = 30$. Hence abc generates G.

(2) How were the mathematical careers of Galois and Cauchy affected by the politics of their time?

There are many ways to answer this but any answer should note at least the following:

- Galois was a fervent Republican during the period of the Bourbon Restoration. His mathematics was repeatedly interrupted by his political provocations. He perceived any professional setback in his brief life as a conspiracy by reactionary forces.

- Cauchy was a royalist and an ardent Catholic throughout his long career, which was repeatedly buffeted by political turmoil: revolution, republic, military coup, and more. At times his faith was in sync with the political order, but very often it was sharply at odds with it.

Quiz 14: 20 April

(1) Let $g = (123)$ and $h = (132)$. Is g conjugate to h in S_4? Justify your answer!

Yes: $(23)(123)(23) = (132)$.

(2) For the same g and h as above: Is g conjugate to h in A_5? Justify your answer!

Yes: $(23)(45)(123)(23)(45) = (132)$.

(3) List all the conjugacy classes of D_6. (You *do not* have to justify your answer.)

If $D_6 = \langle r, s\rangle$ where $r^6 = s^2 = e$ and $srs = r^5$ then the conjugacy classes are $\{e\}$, $\{r^3\}$, $\{r, r^5\}$, $\{r^2, r^4\}$, $\{s, sr^2, sr^4\}$, and $\{sr, sr^3, sr^5\}$.

(4) Find a normal subgroup of order 3 in D_6. (You *do not* have to justify your answer.)

The only subgroup of order 3 in D_6 is $\langle r^2\rangle = \{e, r^2, r^4\}$, which is normal.

(5) Let K denote the normal subgroup from the previous problem. Is the quotient group D_6/K is nonabelian? Explain!

No: The quotient group has order $12/3 = 4$, and every group of order 4 is abelian.

Another way to see this is to observe that every coset xK has order 2 in D_6/K. Any group with this property is abelian, as we proved in exercise 4.6.

Quiz 15: 27 April

Recall that if G is a group and $H < G$ then G acts on G/H by $g(xH) = (gx)H$.

(1) Show that G is transitive on G/H.

We must show that given xH and yH we can find a $g \in G$ such that $g(xH) = yH$. For this we may take $g = yx^{-1}$.

(2) What is the stabilizer in G of the coset H?

The stabilizer of H is the set of all $g \in G$ such that $gH = H$. To say that $gH = H$ is to say that $g \in H$. Hence the stabilizer is precisely the subgroup H.

(3) *Extra credit:* Show that if H is finite then the fixed points for H are those cosets xH such that $xH = Hx$.

A fixed point for H is a coset xH with the property that $hxH = xH$ for every $h \in H$. To say that $hxH = xH$ is to say that $x^{-1}hx \in H$. If this is true for all $h \in H$ then $x^{-1}Hx \subset H$. Since H is finite and conjugation preserves order we conclude that $x^{-1}Hx = H$, whence $Hx = xH$, as claimed.