George M. Bergman Spring 2000, Math 113, Section 3 20 May, 2000
60 Evans Hall **Final Exam** 12:30-3:30 PM

**1.** (44 points, 4 points apiece) Find the following. Correct answers will get full credit whether or not work is shown.

(a) An expression for the permutation $\begin{pmatrix}1\,2\,3\,4\,5\,6\\1\,3\,5\,6\,2\,4\end{pmatrix} \in S_6$ as a product of disjoint cycles.

(b) The number of generators of the multiplicative group of $\mathbb{Z}_{19}$.

(c) $(\mathbb{Z}:10\mathbb{Z})$.

(d) The orbit $S_5 1$, where $S_5$ acts on $\{1,2,3,4,5\}$ by $\sigma i = \sigma(i)$.

(e) A Sylow 3-subgroup of $S_4$.

(f) $\varphi_{\sqrt{2}}(x^3+3x^2-2x)$, where $\varphi_{\sqrt{2}}\colon \mathbb{Q}[x] \to \mathbb{R}$ is the evaluation homomorphism determined by $\sqrt{2}$.

(g) The kernel of the homomorphism $\gamma\colon \mathbb{Q}[x] \to \mathbb{Q}[x]/\langle x^2+2\rangle$, where $\gamma(f(x)) = f(x) + \langle x^2+2\rangle$.

(h) A maximal ideal of $\mathbb{Z}$ containing $45\mathbb{Z}$.

(i) The set of units of $\mathbb{Q}[x]$.

(j) A basis for $\mathbb{Q}[\alpha]$ as a vector space over $\mathbb{Q}$, where $\alpha$ is a complex number whose irreducible polynomial over $\mathbb{Q}$ is $x^8+6$.

(k) A finite field containing a primitive 8th root of unity.

**2.** (30 points; 6 points each) Define each of the following concepts. (You are only asked for the *definitions*, not for facts about these concepts, or examples.)

(a) An **equivalence relation** on a set $X$.

(b) A **normal subgroup** $N$ of a group $G$. (You do not have to define *subgroup*.)

(c) An **action** of a group $G$ on a set $X$.

(d) A **prime ideal** $N$ of a ring $R$. (You do not have to define *ideal*.)

(e) The **degree** $[E:F]$ of a finite extension $E$ of a field $F$.

**3.** (26 points) Below, I prove a theorem and a corollary. Several steps in the proof are shown in italics, with numbers before them. In each case, on the corresponding lines at the bottom of the page, you should give a brief *reason* why the assertion is true: either a general fact (you don't have to specify its theorem-number in Fraleigh!) or an observation about the given situation. Do not worry about giving further reasons to support your reasons; one key fact or calculation is what is wanted in each case. Note also that if you can't justify some step asked for, you can still assume it in justifying later steps.

**THEOREM.** Let $m$ and $n$ be integers such that neither $m$, nor $n$, nor $mn$ is a square in $\mathbb{Z}$. Let $\sqrt{m}$ and $\sqrt{n}$ be square roots of $m$ and $n$ in $\mathbb{C}$. Then $[\mathbb{Q}(\sqrt{m}, \sqrt{n}):\mathbb{Q}] = 4$.

PROOF. Since $m$ has no square root in $\mathbb{Z}$, the polynomial $x^2 - m$ is irreducible over $\mathbb{Z}$, hence it is irreducible over $\mathbb{Q}$. (i) *It follows that* $\mathbb{Q}(\sqrt{m})$ *has degree* 2 *over* $\mathbb{Q}$. (ii) *Hence every element of* $\mathbb{Q}(\sqrt{m})$ *can be written* $a + b\sqrt{m}$ *for* $a, b \in \mathbb{Q}$.

We now claim that $n$ has no square root in $\mathbb{Q}(\sqrt{m})$. Indeed, suppose we had $(a + b\sqrt{m})^2 = n$ $(a, b \in \mathbb{Q})$. (iii) *Expanding out, we see that* $a$ *or* $b$ *must be* 0. If $b$ were 0, that would make $a^2 = n$, so $n$ would have a square root in $\mathbb{Q}$, so $x^2 - n$ would be reducible over $\mathbb{Q}$, hence over $\mathbb{Z}$, contradicting our assumption that $n$ is not a square in $\mathbb{Z}$. On the other hand, if $a$ were 0, we would have $mb^2 = n$. Multiplying both sides by $m$, we see that $mn$ would be a square in $\mathbb{Q}$, which similarly contradicts our assumption that it is not a square in $\mathbb{Z}$. These contradictions show that $n$ indeed has no square root in $\mathbb{Q}(\sqrt{m})$, so $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ has degree 2 over $\mathbb{Q}(\sqrt{m})$. (iv) *It follows that* $[\mathbb{Q}(\sqrt{m}, \sqrt{n}):\mathbb{Q}] = 4$. □

**COROLLARY.** For $m$ and $n$ as in the preceding theorem, $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ is a simple extension of $\mathbb{Q}$, generated by the element $\sqrt{m} + \sqrt{n}$.

PROOF. Recall that a conjugate of an element of an extension field means an element which has the same irreducible polynomial. (v) *We see from the proof of the preceding theorem that* $-\sqrt{n}$ *is a conjugate of* $\sqrt{n}$ *over* $\mathbb{Q}(\sqrt{m})$. Hence there is an automorphism $\psi_{\sqrt{n},-\sqrt{n}}$ of $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ which fixes $\mathbb{Q}(\sqrt{m})$ and takes $\sqrt{n}$ to $-\sqrt{n}$. Reasoning in the same way with the roles of $m$ and $n$ reversed, there is likewise an automorphism $\psi_{\sqrt{m},-\sqrt{m}}$ of $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ which fixes $\mathbb{Q}(\sqrt{n})$ and takes $\sqrt{m}$ to $-\sqrt{m}$. Now $\sqrt{m} + \sqrt{n}$ is carried by $\psi_{\sqrt{n},-\sqrt{n}}$ to $\sqrt{m} - \sqrt{n}$, by $\psi_{\sqrt{m},-\sqrt{m}}$ to $-\sqrt{m} + \sqrt{n}$, and by their composite to $-\sqrt{m} - \sqrt{n}$. (vi) *Hence* $\sqrt{m} - \sqrt{n}$, $-\sqrt{m} + \sqrt{n}$, *and* $-\sqrt{m} - \sqrt{n}$ *are conjugates of* $\sqrt{m} + \sqrt{n}$. (vii) *It follows that the irreducible polynomial of* $\sqrt{m} + \sqrt{n}$ *must have degree at least* 4.

Thus $[\mathbb{Q}(\sqrt{m} + \sqrt{n}):\mathbb{Q}] \geq 4$. (viii) *Comparing degrees, we see that* $\mathbb{Q}(\sqrt{m} + \sqrt{n}) = \mathbb{Q}(\sqrt{m}, \sqrt{n})$, *as desired.* □