Name ______________________________

Algebra I Final Exam - Spring 2007

(1) For each of the following examples, find the splitting field K of the polynomial $f(x)$ over the field F. Find $\mathrm{Gal}(K/F)$ and find all subfields of K which contain F. Indicate which of these subfields are contained in each other by drawing the inclusion lattice.

(a) $F = \mathbf{Q}$, $f(x) = x^4 - 7$
(b) $F = \mathbf{Q}$, $f(X) = x^4 - 49$
(c) $F = \mathbf{F}_2$, $f(x) = x^{4096} - x$
(d) $F = \mathbf{Q}(e^{2\pi i/10})$, $f(x) = x^{10} - 5$

(2) (a) Prove that the ring $R = \mathbf{Z}[\sqrt{3}]$ is a Unique Factorization Domain.
(b) Prove that $1 + 2\sqrt{3}, 4 + \sqrt{3}, 8 + 5\sqrt{3}$, and $11 + 6\sqrt{3}$ are all prime in R.
(c) Note that

$$(4 + \sqrt{3})(8 + 5\sqrt{3}) = 47 + 28\sqrt{3} = (11 + 6\sqrt{3})(1 + 2\sqrt{3}).$$

Explain.

(3) (a) List (up to isomorphism) all the abelian groups of size 180.
(b) Let N be the subgroup of $\mathbf{Z}^3$ generated by the vectors $(7, 14, 24), (1, 0, -4)$, and $(4, 6, 8)$. Find the invariant factors of the quotient group $\mathbf{Z}^3/N$.

(4) Let R be a ring and let M be an R-module. Let I be an ideal of R. Define

$$IM = \{\alpha m : \alpha \in I, m \in M\}.$$

(a) Prove that IM is an R-submodule of M.
(b) Suppose that N is another R-module and that $\phi\colon M \to N$ is an R-module homomorphism. Prove that ϕ induces an R-module homomorphism from $M/IM \to N/IN$ such that the obvious diagram commutes.
(c) Do problem 13 in Chapter 10.2.

(5) This problem will investigate the roots and splitting field of the polynomial $f(x) = x^4 - 22x^2 + 1$.

(a) What are the 4 roots of $f(x)$? Prove that they are all constructible via compass and straight-edge.
(b) Let α be a root of $f(x)$. Prove that $\frac{1}{\alpha}$ is also a root.

(c) Prove that $\mathbf{Q}(\alpha)$ is the splitting field of $f(x)$ over $\mathbf{Q}$.
(d) Write down the elements of $\mathrm{Gal}(\mathbf{Q}(\alpha)/\mathbf{Q})$ as permutations of the 4 roots of $f(x)$.
(e) What group of size 4 is this?
(f) How many subfields of $\mathbf{Q}(\alpha)$ have dimension 2 over $\mathbf{Q}$? Prove that $\mathbf{Q}(\alpha + \frac{1}{\alpha})$ is one of them.
(g) We've seen that a field having dimension 2 over $\mathbf{Q}$ must be of the form $\mathbf{Q}(\sqrt{d})$ for some rational number d. (Indeed, d can always be chosen to be a squarefree integer.) Express each of the dimension 2 subfields of $\mathbf{Q}(\alpha)$ in this form.

(6) Do problems 21 and 26 in Chapter 14.2 and problem 9 in chapter 14.7.