بسمه تعالی

دانشگاه صنعتی شریف
دانشکدهٔ علوم ریاضی

آزمون ورودی دورهٔ دکتری ریاضی

تاریخ امتحان: **جمعه ۸۳/۳/۱**
موضوع امتحان: **نظریه اعداد**

همهٔ مسائل ارزش برابر دارند.

۱– اگر q, p دو عدد اول باشند و داشته باشیم $p = ۴q + ۱$، نشان دهید ۲ یک ریشهٔ اولیه به پیمانهٔ p است.

۲– فرض کنید F میدانی با مشخصهٔ p، E گسترشی جبری از F و $\alpha \in E$ باشد. نشان دهید α روی F جدایی‌پذیر است اگر و تنها اگر برای هر $n \geq ۱$ داشته باشیم $F(\alpha^{p^n}) = F(\alpha)$.

۳– فرض کنید F میدان شکافندهٔ چندجمله‌ای $f(x) = x^۴ - ۲$ روی $\mathbb{Q}$ و G گروه گالوای F روی $\mathbb{Q}$ باشد. اولاً مرتبهٔ G را محاسبه کنید و ثانیاً مشخص کنید که G با کدام گروه معروف یکریخت است.

۴– الف) نشان دهید $\mathbb{Z}[\sqrt{-۲}]$ حوزه‌ای اقلیدسی است.

ب) معادلهٔ $y^۲ = x^۳ - ۲$ را (با $x, y \in \mathbb{Z}$) حل کنید.

۵– عدد رده‌ای $\mathbb{Q}(\sqrt{-٦})$ را محاسبه کنید.

٦– فرض کنید a و b دو عدد صحیح مثبت و فرد باشند، به‌طوری که $b^۲ < \frac{۳^a}{۲}$. اگر عدد $c = ۳^a - b^۲$ خالی از مربع باشد، نشان دهید که در گروه رده‌های ایده‌آلی میدان $\mathbb{Q}(\sqrt{-c})$ عنصری از مرتبهٔ a وجود دارد.

Sharif University of Technology

Department of Mathematical Sciences

Ph.D. Entrance Examination
Number Theory

1) Let p, q be two prime numbers with $p = 4q + 1$. Show that 2 is a primitive root mod p.

2) Let F be a field of characteristic p, E an algebraic extension of F, and $\alpha \in E$. Show that α is separable over F if and only if $F(\alpha^{p^n}) = F(\alpha)$ for all $n \geq 1$.

3) Let F be the splitting field of the polynomial $f(x) = x^4 - 2$ over $\mathbb{Q}$, and G be the Galois group of $F/\mathbb{Q}$. Compute the order of G and find a well-known group isomorphic to G.

4) a) Show that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.

b) Solve the equation $y^2 = x^3 - 2$ (with $x, y \in \mathbb{Z}$).

5) Find the class number of $\mathbb{Q}(\sqrt{-6})$.

6) Let a, b be odd positive integers such that $b^2 < \dfrac{3^a}{2}$. If $c = 3^a - b^2$ is square-free, show that the ideal-class group of the field $\mathbb{Q}(\sqrt{-c})$ contains an element of order a.