Math 30820 Honors Algebra 4
Homework 1

Andrei Jorza

Due Wednesday, 1/25/2017

Do 4 of the following questions. Some questions may be obligatory. Artin a.b.c means chapter a, section b, exercise c. You may use any problem to solve any other problem.

1. Determine, with proof, the minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$.

   Proof. If $\alpha=\sqrt{2}+\sqrt{3}$ then $(\alpha-\sqrt{2})^2=3$ and so $\alpha^2-1=2\alpha\sqrt{2}$ which immediately implies that α is a root of $P(X)=X^4-10X^2+1$. We need to show this is irreducible over $\mathbb{Q}$. If it were reducible it would be of the form $P(X)=A(X)B(X)$. If $\deg A=1$ this would imply that P has a rational root, but the roots of P are $\pm\sqrt{2}\pm\sqrt{3}$ which are not rational. Indeed, if this were the case, we'd get that $\mathbb{Q}(\sqrt{2})=\mathbb{Q}(\sqrt{3})$ and we saw last semester that these two are not isomorphic as rings. The only other option is $\deg A=\deg B=2$. But this would imply that the roots of A add up to a rational. But pairwise sums of roots of P are $\pm 2\sqrt{2}$, $\pm 2\sqrt{3}$ and 0. The only option is if A has roots $\pm(\sqrt{2}+\sqrt{3})$ and B has roots $\pm(\sqrt{2}-\sqrt{3})$. But then the roots of A multiply out to $5+2\sqrt{6}$ which is not rational.

   Alternatively, A and B can be chosen in $\mathbb{Z}[X]$ by Gauss' lemma. Then they'd have to be monic as P is. So $A=X^2+aX+b$ and $B=X^2+cX+d$. Multiplying out we'd get $c=-a$ and $bd=1$. But then $P=AB=(X^2+b)^2-a^2X^2$ so we'd need $2b-a^2=-10$. Since $b=\pm 1$ we immediately get that there is no $a\in\mathbb{Z}$ satisfying the equation. □

2. Determine, with proof, the minimal polynomial of $\sqrt{2+\sqrt{2+\sqrt{2}}}$ over $\mathbb{Q}$.

   Proof. As before the element satisfies the polynomial $P(X)=((X^2-2)^2-2)^2-2$. Expanding we immediately apply Eisenstein with $p=2$. □

3. Determine, with proof, the minimal polynomial of the element $\sqrt{X+\sqrt[p]{X}}$ over the PID $\mathbb{F}_p[X]$. Here p is a prime and $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$.

   Proof. The element $\alpha=\sqrt{X+\sqrt[p]{X}}$ satisfies the polynomial $P(Y)=(Y^2-X)^p-X$. We're in characteristic p and from last semester we know that $x\mapsto x^p$ is a ring homomorphism in this case so $P(Y)=Y^{2p}-X^p-X$. In Eisenstein we choose the prime $X\in\mathbb{F}_p[X]$. Then $X\mid -X^p-X$ but $X^2\nmid -X^p-X$ so $P(Y)$ must be irreducible. □

4. (Generalized Eisenstein criterion) Suppose R is a unique factorization domain and $\mathfrak{p}$ is a prime ideal of R such that $R/\mathfrak{p}$ is also a unique factorization domain. Let $P(X)\in R[X]$ be $P(X)=X^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0$. Show that if $a_0,\ldots,a_{n-1}\in\mathfrak{p}$ but $a_0\notin\mathfrak{p}^2$ then $P(X)$ is irreducible in $R[X]$ (and therefore also in $(\operatorname{Frac} R)[X]$ by Gauss' lemma from last semester).

Proof. Consider $\pi : R \to R/\mathfrak{p}$ be the natural ring homomorphism $\pi(x) = x \mod \mathfrak{p}$. Then $\pi : R[X] \to R/\mathfrak{p}[X]$ is also a ring homomorphism. If P were reducible, say, $P(X) = A(X)B(X)$ then $\pi(P) = \pi(A)\pi(B)$. But $\pi(P) = X^n$ by assumption and so $\pi(A)\pi(B) = X^n$. Since $R/\mathfrak{p}$ is a UFD so is $R/\mathfrak{p}[X]$ and therefore $\pi(A) = X^k$ and $\pi(B) = X^{n-k}$ for some k between 1 and $n-1$. But then $A(X) - X^k \in \mathfrak{p}[X]$ and $B(X) - X^{n-k} \in \mathfrak{p}[X]$ and so $A(0), B(0) \in \mathfrak{p}$. But then $P(0) = A(0)B(0) \in \mathfrak{p}^2$ contradicting the assumption. □

5. Suppose $R \subset S$ are rings. An element $\alpha \in S$ is said to be *integral over* R if $P(\alpha) = 0$ for some **monic** polynomial $P \in R[X]$. Suppose R is a unique factorization domain. Show that if $\alpha \in \operatorname{Frac} R$ is integral over R then $\alpha \in R$.

   Proof. Write $\alpha = a/b$ with $b \neq 0$ and $a, b \in R$ coprime. Suppose α satisfies the monic equation

   $$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

   with $a_i \in R$. Clearing denominators we get

   $$a^n + a_{n-1}a^{n-1}b + \cdots + a_1 ab^{n-1} + a_0 b^n = 0$$

   which implies $b \mid a^n$. If b is a unit then $\alpha = a/b \in R$. Otherwise let π be a prime factor of b. Then $\pi \mid a^n$ so $\pi \mid a$ by primality, which contradicts the assumption that a and b are coprime. □

6. Suppose α is integral over a ring R. Show that $R[\alpha]$ (defined last semester as $\{P(\alpha) \mid P \in R[X]\}$) is in fact the set $\{a_0 + a_1\alpha + \cdots + a_n\alpha^n \mid a_0, \ldots, a_n \in R\}$ for some integer n.

   Proof. Let $P(X) = X^{n+1} + b_n X^n + \cdots + b_1 X + b_0$ be a polynomial such that $P(\alpha) = 0$. Denote $\mathcal{S} = \{a_0 + a_1\alpha + \cdots + a_n\alpha^n \mid a_0, \ldots, a_n \in R\}$ and note that $\mathcal{S}$ is closed under addition. Then $\alpha^{n+1} = -(b_n\alpha^n + \cdots + b_1\alpha + b_0) \in \mathcal{S}$. We need to show that $Q(\alpha) \in \mathcal{S}$ for every $Q \in R[X]$. Suppose this is not the case. Let Q be a polynomial of smallest degree such that $Q(\alpha) \notin \mathcal{S}$. Clearly $\deg Q > n$ as $\mathcal{S}$ is defined to be the image under evaluation at α of polynomials of degree $\leq n$. Say $Q(X) = q_m X^m + \cdots + q_1 X + q_0$ has degree $m > n$ and write $R(X) = Q(X) - q_m X^m$ with degree $\deg R < \deg Q$. Then

   $$Q(\alpha) = q_m\alpha^m + R(\alpha)$$

   By choice of Q and the fact that $\deg R < \deg Q$ we know $R(\alpha) \in \mathcal{S}$. Since $Q(\alpha) \notin \mathcal{S}$ and $\mathcal{S}$ is closed under addition we deduce that $a_m\alpha^m \notin \mathcal{S}$. But

   $$q_m\alpha^m = q_m\alpha^{m-n-1}\alpha^{n+1} = -q_m(b_n\alpha^{m-1} + b_{n-1}\alpha^{m-2} + \cdots + b_0\alpha^{m-n-1})$$

   and the RHS is a polynomial in α of degree $m - 1 < \deg Q$ and so lies in $\mathcal{S}$. This is a contradiction. □