Algebra II, Spring 2017

Solutions to Problem Set 7

1. (a) Let M be the collection of all ideals of A containing I whose intersection with S is empty. Then M is non-empty since $I \in M$. On the other hand every increasing chain of ideals in M has a maximal element (their union), so M has a maximal element J be Zorn's lemma. We claim that J is a prime ideal. If $ab \in J$ and $a \notin J$ and $b \notin J$, then the ideal J_1 generated by J and x can not belong to M (by maximality of J), so it intersects S, so there is $x \in A$ and $j_1 \in J$ such that $xa + j_1 = s_1 \in S$. Similarly, there is $y \in A$ and $j_2 \in J$ such that $yb + j_2 = s_2 \in S$. Then $s_1 s_2 \in S$ since S is multiplicatively closed, and

$$s_1 s_2 = xaj_1 + ybj_2 + xy(ab) + j_1 j_2 \in J,$$

a contradiction.

(b) Clearly, $rad(I)$ is contained in every prime ideal containing I. Conversely, if a is contained in every prime ideal containing I, and no power of a is in I, then $S = \{1, a, \ldots, a^n, \ldots\}$ is a multiplicative subset of A, and by part (a), there is a prime ideal $\mathfrak{p}$ such that $I \subset \mathfrak{p}$ and $\mathfrak{p} \cap S = \emptyset$, so $a \notin \mathfrak{p}$, a contradiction.

2. Suppose $\mathfrak{m} = rad(I)$ where $\mathfrak{m}$ is a maximal ideal. Then by Question 1, the only prime (and in particular maximal) ideal which contains I in $\mathfrak{m}$. If $y^n \notin I$ for every $n \geq 1$, then $y \notin \mathfrak{m} = rad(I)$. Let $J = I + (y)$. Then J is an ideal containing I and if it is not equal to A, then it is contained in a maximal ideal $\mathfrak{n}$. But then $\mathfrak{n} \neq \mathfrak{m}$ since $y \in \mathfrak{n}$, which is not possible. So $I + (y) = A$, hence $1 = i + ay$ for some $i \in I$ and $a \in A$. Multiplying by x we get, $x = ix + axy \in I$.

3. In class, we gave an example of a prime ideal $\mathfrak{p}$ such that $\mathfrak{p}^2$ is not primary. We show $rad(\mathfrak{p}^2) = \mathfrak{p}$. We have $\mathfrak{p}^2 \subset \mathfrak{p}$, so

$$\mathfrak{p} \subset rad(\mathfrak{p}^2) \subset rad(\mathfrak{p}) = \mathfrak{p},$$

so $rad(\mathfrak{p}^2) = \mathfrak{p}$.

4. Every ideal in $S^{-1}A$ is of the form $S^{-1}I$ for some ideal $I \subset A$. If I is generated by $a_1, \ldots, a_m$, then $S^{-1}I$ is generated by $\frac{a_1}{1}, \ldots, \frac{a_m}{1}$.

5. We first show f has no rational root. Since $\mathbf{Z}$ is integrally closed in $\mathbf{Q}$, every rational root of f should be an integer. But for every integer x with $|x| \geq 4$, $x^4 - 10x^2 + 1 = x^2(x^2 - 10) + 1 > x^2 + 1 > 0$, and no integer with $|x| \leq 3$ is a root of f either. Suppose now that f is a product of two irreducible factors

$$x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 + dx + c).$$

Then $a + d = 0$, so $d = -a$. Also, $bc = 1$, $bd + ca = 0$, and $ad + b + c = -10$. So $-ab + ca = 0$, so $a = 0$, or $c = b$. And $-a^2 + b + c = -10$. If $a = 0$, then $b + c = -10$ and $bc = 1$ which is not possible since b and c are rational. If $c = b$, then $bc = 1$, so $b = \pm 1$. But then $a^2 = b + c + 10 = 12$ or 8, which is not possible since we are assuming a, b, c are rational.

(b) Let L be the splitting field of f. The roots of f are $\pm\alpha$ and $\pm\beta$ for some $\alpha, \beta \in L$. Since the product of all roots of f is 1, we have $(\alpha\beta)^2 = 1$, so $\alpha\beta = \pm 1$. Let $\sigma \in \mathrm{Gal}(\mathrm{L}/\mathbf{Q})$. We show if $\sigma \neq id$, then σ has order 2.

- If $\sigma(\alpha) = -\alpha$, then $\sigma(\beta) = -\beta$, so $\sigma^2 = id$.
- If $\sigma(\alpha) = \beta$, and $\alpha\beta = 1$, then $\sigma(\alpha)\sigma(\beta) = 1$, so $\sigma(\beta) = 1/\sigma(\alpha) = 1/\beta = \alpha$, so $\sigma^2 = id$. Similarly, if $\alpha\beta = -1$, then $\sigma(\alpha)\sigma(\beta) = -1$, so $\sigma(\beta) = -1/\beta = \alpha$.
- If $\sigma(\alpha) = -\beta$, and $\alpha\beta = 1$, then $\sigma(\beta) = 1/(-\beta) = -\alpha$. Similarly, if $\alpha\beta = -1$, then $\sigma(\beta) = -1/(-\beta) = -\alpha$. So in this case, $\sigma^2 = id$ too.

Therefore the Galois group is isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$.

(c) If $p = 2$, then $f(x) = x^4 + 1 = (x^2 + 1)^2 \mod 2$. If $p = 3$, then

$$x^4 - 10x^2 + 1 = (x^2 + 1)^2 \mod 3$$

So assume $p \neq 2, 3$. Then $f' = 4x^3 - 20x = 4x(x^2 - 5)$, so f and f' has no common roots (since if α is a common root of f and $f' \mod p$ in the algebraic closure of $\mathbf{F}_p$, then $\alpha^2 = 5$, so $f(\alpha) = \alpha^2(\alpha^2 - 10) + 1 = -24$ so $p = 2$ or $p = 3$.) This shows that f has no repeated roots. Let K be the splitting field of $f \mod p \in \mathbf{F}_p[x]$, and assume $f \mod p$ is irreducible. Then $[K : \mathbf{F}_p] \geq 4$, and also since the Galois group of every finite extension of $\mathbf{F}_p$ is cyclic, $\mathrm{Gal}(\mathrm{K}/\mathbf{F}_\mathrm{p})$ contains an n-cycle $n \geq 4$. This is not possible since $\mathrm{Gal}(\mathrm{L}/\mathbf{Q})$ has no 4-cycle.